U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7264
BNL-228841-2025-NREG

Managing the Effects of Degraded Digital Instrumentation and Control Conditions on Operator Performance

Human Factors Engineering Review Guidance Development

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Library at www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources:

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Washington, DC 20402-0001
   Internet: https://bookstore.gpo.gov/
   Telephone: (202) 512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22312-0002
   Internet: https://www.ntis.gov/
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: **U.S. Nuclear Regulatory Commission**
Office of Administration
Program Management and Design Service Branch
Washington, DC 20555-0001
E-mail: Reproduction.Resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
Internet: https://www.ansi.org/
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX),(4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and the Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of the NRC's regulations (NUREG-0750), (6) Knowledge Management prepared by NRC staff or agency contractors (NUREG/KM-XXXX).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7264
BNL-228841-2025-NREG

Managing the Effects of Degraded Digital Instrumentation and Control Conditions on Operator Performance

Human Factors Engineering Review Guidance Development

Manuscript Completed: May 2025
Date Published: December 2025

Prepared by:
J. O'Hara[1], W. Gunther[1]
G. Martinez-Guridi[1], T. Anderson[1]
J. Xing[2], S. Morrow[2]

[1]Brookhaven National Laboratory,
Upton, NY

[2]U.S. Nuclear Regulatory Commission
Washington, DC

Jing Xing and Stephanie Morrow, NRC Project Managers

Office of Nuclear Regulatory Research

ABSTRACT

Modern digital instrumentation and control (DI&C) systems provide sophisticated monitoring, diagnostic, and prognostic functions, as well as integrated control of plant systems and processes. Personnel interact with DI&C systems through human-system interfaces (HSIs) in the control room and elsewhere in a nuclear power plant. While digital systems are generally reliable, their potential degradation or failure could affect operator performance and consequently impact plant safety.

The objectives of this U.S. Nuclear Regulatory Commission (NRC) research were to (1) examine the effects of degraded HSI and DI&C conditions on human performance and plant operations, and (2) develop guidance for the review of HSI support for the detection and management of degraded HSI and DI&C conditions by plant personnel. The study followed the NRC's methodology for the development of human factors engineering guidance, which consists of four steps: (1) user needs analysis, (2) technical basis and guidance development, (3) peer review, and (4) guidance integration and document publication. The technical basis was established from a review of pertinent standards and guidelines, empirical studies, plant operating experience, and DI&C failure events. The guidance in this report was incorporated into NUREG-0700, Revision 3, "Human-System Interface Design Review Guidelines," issued July 2020.

FOREWORD

An earlier draft of this report was published in 2010 as Brookhaven National Laboratory (BNL) Technical Report No. 91047-2010, "The Effects of Degraded Digital Instrumentation and Control Systems on Human-System Interfaces and Operator Performance." Subsequent revisions and updates were made to the report, and the U.S. Nuclear Regulatory Commission (NRC) incorporated the modified guidance into Revision 3 of NUREG-0700, "Human-System Interface Design Review Guidelines," issued July 2020. The NRC human factors staff decided to release this revised report as a NUREG/CR for knowledge management, as it thoroughly describes the process for developing human factors engineering (HFE) guidance. The report covers a topic of continued importance for nuclear safety—detecting and managing degraded digital instrumentation and control (DI&C) conditions—as the nuclear industry sees greater use of digital control rooms and automation of safety functions.

At the time of this publication, the NRC is engaged in preapplication activities with vendors proposing new and advanced reactor designs that will likely use fully digital control rooms. In addition, modernization activities at operating plants include greater use of digital systems and automation in the control room. As use of DI&C increases, so does the level of integration among plant systems, as well as integration between plant systems and human operators. It is important that vendors and regulators bring together different aspects of their design and review processes in order to account for the interrelationships in the areas of DI&C and HFE, in view of their role in ensuring safety.

The NRC has taken steps to prepare for licensing activities associated with modernized and advanced reactors, as laid out in the roadmap for review of advanced reactor applications, DANU-ISG-2022-01, "Review of Risk-Informed, Technology-Inclusive Advanced Reactor Applications—Roadmap." These activities necessarily include consideration of DI&C and HFE. Modernization efforts may involve replacing analog instrumentation and control with DI&C, as well as automating activities that were once performed manually. Regarding modernization of operating plants, DI&C-ISG-06, Revision 2, "Digital Instrumentation and Controls: Licensing Process," issued December 2018, contains interim staff guidance (ISG) for reviewing license amendment requests (LARs) associated with safety-related DI&C equipment modifications in operating plants and in new plants once they become operational. DI&C-ISG-06 indicates that, for modifications that may involve HFE considerations, "an HFE safety evaluation should be performed in accordance with SRP [NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition] Chapter 18, 'Human Factors Engineering'; NUREG-0711, 'Human Factors Engineering Program Review Model'; and NUREG-1764, 'Guidance for the Review of Changes to Human Actions,' with close coordination with the DI&C evaluation under SRP Chapter 7 [Instrumentation and Controls]."

This report presents a framework for characterizing the interrelated aspects of DI&C, human-system interfaces (HSIs), and human performance. The framework brings together considerations related to DI&C and HFE in degraded instrumentation and control (I&C) conditions and provides a foundation for the guidelines on detecting and managing degraded I&C conditions that were incorporated into Revision 3 of NUREG-0700. The development of these guidelines was an initial effort by the NRC to integrate review activities in the areas of DI&C and HFE. The U.S. nuclear industry has also been working to integrate these areas. For example, the Electrical Power Research Institute (EPRI) report "Digital Engineering Guide:

Decision Making Using Systems Engineering" includes DI&C requirements, HFE, and human reliability analysis within the same framework in the design process.

Another contribution of this report is that it systematically documents the NRC's methodology for developing HFE guidance. The methodology consists of four high-level steps: (1) user needs analysis, (2) technical basis and guidance development, (3) peer review, and (4) guidance integration and document publication. Section 2 of this report describes in detail each step in the methodology. The remainder of the report demonstrates how the guidance development methodology was applied to the topic of operation under degraded HSI and I&C conditions. The novel concepts of operation anticipated for advanced reactors will give rise to new needs for HFE guidance development, and this report provides a roadmap for effectively using research to develop licensing review guidance for the NRC staff.

The NRC human factors staff would like to express sincere appreciation to Dr. John O'Hara, the primary author of this report and many other seminal publications on HFE in the nuclear industry. His work has been integral to the nuclear industry's incorporation of human factors principles into its design processes to ensure the safe operation of nuclear power plants.

Stephanie Morrow and Jing Xing

Human Factors and Reliability Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

May 2025

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The designs of new and advanced nuclear power plants (NPPs) differ from those of currently operating plants in many respects. One important difference is their use of digital instrumentation and control (DI&C) systems. Instrumentation and control (I&C) systems are used to set basic parameters, monitor plant processes, and control various barriers that support plant safety. They also respond to transients, accidents, and other failure events. While new and advanced reactors are the predominant users of DI&C, operating reactors are also undergoing digital upgrades, which are essential for light-water reactor sustainability.

An I&C system is made up of sensors, logic and algorithms, and subsystems for monitoring, automation, and communication. Although digital technology is expected to improve system performance, it also poses new challenges. Increases in sensing capabilities, information processing support, intelligent agents, automation, and software-mediated interfaces create opacity between personnel and the physical plant. They also add complexity to the tasks of personnel operating and maintaining the plant.

Moreover, throughout their life cycle, I&C systems undergo degradation, meaning that systems or components may operate differently or less effectively than intended, and they may even fail. I&C degradation may cause unexpected operating conditions and severely affect human performance, possibly threatening plant safety. Digital technology gives rise to numerous factors that may contribute to DI&C degradation, including, but not limited to, engineering errors due to increasing functionality, complexity in software and control logic, uncertainty in the verification and validation process, and faults resulting from maintenance, upgrades, and configuration changes.

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research sponsored the research in this report to investigate the effects of I&C system degradation on human performance and plant operations. The objective of the research was to develop guidance for human factors engineering (HFE) reviews addressing the operator's ability to detect and manage degraded DI&C conditions. The research included the review of pertinent standards and guidelines, empirical studies, and plant operating experience, as well as an evaluation of how selected failure modes of a digital feedwater system might affect human-system interfaces and operator performance. The research also included development of a conceptual framework characterizing the relationship between I&C systems, human-system interfaces, and human performance, which may support future analysis to generalize the effects of degraded I&C conditions.

The research findings indicate that degradation of DI&C systems is not uncommon and may significantly affect the overall behavior of a plant, for example, by causing a reactor to trip or equipment to operate unexpectedly. Various modes of DI&C degradation may affect the human-system interfaces used by operators to monitor and control the plant. For example, deterioration of the sensors can complicate the operators' interpretation of information and sometimes mislead operators about plant conditions. The potential impacts of degraded I&C on human performance include the following:

- poor situation awareness due to degradation of sensors and monitoring subsystems

- poor situation awareness and response planning due to degradations of automatic systems
- effects on workload and teamwork, as the failure of automation may require personnel to manually perform tasks that were previously automated
- unstable operator action due to communication subsystem delays and system malfunctions or failures

One outcome of this research was the development of HFE review guidance for the NRC staff to use in assessing the adequacy of a licensee's or applicant's approach to addressing the detection and management of degraded I&C conditions. The framework and guidelines developed in this research have been applied in HFE reviews and incorporated into NUREG-0700, Revision 3, "Human-System Interface Design Review Guidelines," issued July 2020.

This report establishes the technical basis and guidance for detecting and managing degraded I&C conditions. It also presents the NRC's methodology for developing HFE guidance. The report supports regulatory decision-making by elucidating the potential human performance issues associated with DI&C system degradation. This information can be used to improve human performance and plant safety as new DI&C systems are introduced in NPPs. The findings presented in this report encourage continued research on human factor considerations related to emerging technologies being used in NPPs, as well as incorporation of the results of such research into regulatory guidance.

ACKNOWLEDGMENTS

The authors thank Val Barnes, Stephen Fleger, Paul Pierringer, and Ismael Garcia of the U.S. Nuclear Regulatory Commission (NRC) and Jim Higgins of Brookhaven National Laboratory for their insights and helpful comments on all aspects of this report.

ABBREVIATIONS

A/M	auto/manual
ATHEANA	A Technique for Human Event Analysis
B/U	backup
BCPU	backup central processing unit
BFRV	bypass feedwater regulating valve
BFV	bypass feedwater valve
BIT	boron injection tank
BNL	Brookhaven National Laboratory
BTP	branch technical position
CBP	computer-based procedure
CFR	*U.S. Code of Federal Regulations*
CPU	central processing unit
DEV	deviation
DFWCS	digital feedwater control system
DI&C	digital instrumentation and control
DOE	U.S. Department of Energy
DPI	direct perception interface
DURESS	Dual Reservoir System Simulation
ECCS	emergency core cooling system
EDG	emergency diesel generator
EID	ecological interface design
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERDADS	emergency response data acquisition and display system
FMEA	failure modes and effects analysis
FTA	fault tree analysis
FWP	feedwater pump
HAZCADS	Hazards and Consequences Analysis for Digital Systems
HFE	human factors engineering
HRA	human reliability analysis
HSI	human-system interface
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
ICHSI	instrumentation, control, human-system interface
IEEE	Institute of Electrical and Electronics Engineers
IN	information notice
ISG	interim staff guidance
LAR	license amendment request

LER	licensee event report
MCPU	main central processing unit
MFRV	main feedwater-regulating valve
MFV	main feedwater valve
MUX	multiplexer
NEI	Nuclear Energy Institute
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
OHA	overhead annunciator
P	physical (interface)
P+F	physical plus functional (interface)
PC	plant computer
PDI	pressure differential indication
PDU	plasma display unit
PID	piping and instrumentation display
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PWR	pressurized-water reactor
RCIC	reactor core isolation cooling
RG	regulatory guide
RIS	regulatory issue summary
S/G	steam generator
SI	safety injection
SRP	Standard Review Plan (NUREG-0800)
Std.	standard
STPA	systems-theoretic process analysis
TCT	trial completion time
TR	technical report
VDU	video display unit

1 INTRODUCTION

1.1 Background

The designs of new nuclear power plants (NPPs) differ in many respects from the designs of NPPs that were built in the 1970s and 1980s. One important difference is the digitalization of their instrumentation and control (I&C) systems and human-system interfaces (HSIs). The current fleet of operating NPPs in the United States was predominantly designed and built with analog I&C technology, while new plants employ digital I&C (DI&C) and HSI technologies. The latter offer functions and capabilities that are vital for performance and plant safety.

The I&C system and plant personnel, working together through the HSIs (see Figure 1-1), do the following:

- Sense basic parameters and statuses.
- Control operations.
- Respond to transients, accidents, and other failures.
- Monitor and control plant processes and performance, as well as various barriers that prevent the release of radioactive material.

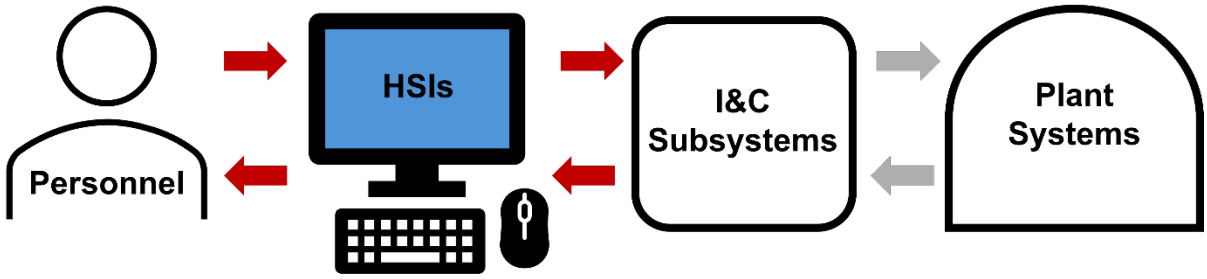


Figure 1-1 A Diagram of Personnel Interaction with the I&C System

Analog HSIs have hardwired controls (e.g., switches, knobs, and handles) and displays (e.g., alarm tiles, meters, linear scales, and indicator lights) arranged on control boards (see Figure 1-2). Operators walk the boards and accomplish their tasks by following paper procedures.

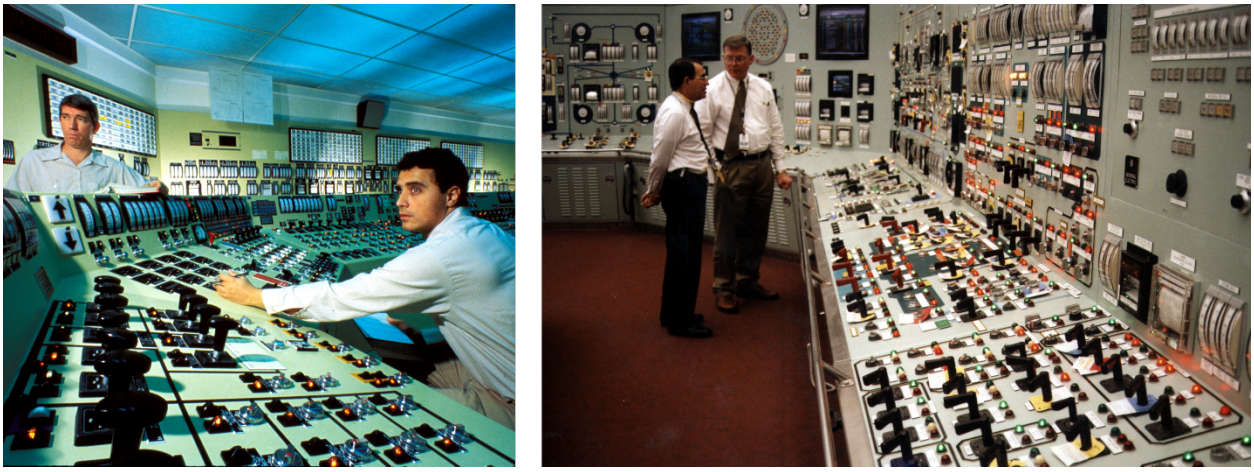


Figure 1-2 Analog HSIs in a NPP Control Room

Many operating U.S. plants are undergoing modernization projects to replace some of their analog I&C systems and HSIs with new digital systems (O'Hara, 2004; O'Hara et al., 2000; Dudenhoeffer et al., 2007; Joe and Kovesdi, 2018; Hunton et al., 2020). Digital modernization efforts have resulted in NPP control rooms with a combination of analog and digital HSIs (see Figure 1-3).

Figure 1-3 Mix of Analog and Digital HSIs in a NPP Control Room

New NPPs have computer-based HSIs organized into sit-down workstations with screen-based displays from which personnel monitor the plant (see Figure 1-4). Onscreen soft controls, accessed through computer workstations, are used to control plant equipment. Large-panel displays are often used to present high-level information to crew members. In digitized control rooms, the procedures may also be computer-based, so that operators can take control actions directly from a procedure display or can authorize the procedure to perform a series of actions (a configuration known as semiautomated control).

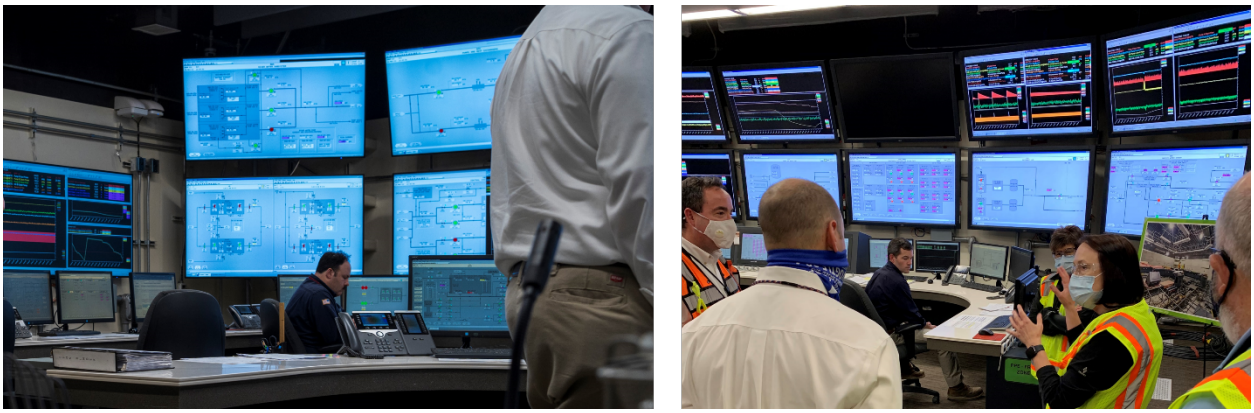


Figure 1-4 Digital HSIs in a NPP Control Room

Modern digital systems perform sophisticated monitoring of equipment conditions and offer both diagnostic and prognostic functions. They can be used to implement control algorithms that are more advanced than those used in plants to date, such as techniques for optimal control, nonlinear control methods, fuzzy logic, neural networks, state-based control, and adaptive control (i.e., controls that modify their behavior based on plant dynamics) (O'Hara et al., 2008b). These advanced techniques enable more intricate and granular control of plant systems and processes. DI&C systems also support increased automation and new forms of automation that make unique interactions between personnel and automatic functions.

Although digital technology can improve operational performance, it also poses certain challenges. Increases in sensing capabilities, information processing support, intelligent agents, automation, and software-mediated interfaces extend the "distance" between personnel and the physical plant. This distance is even more challenging for personnel to navigate when I&C and HSI degradation occurs. Such degradation may significantly reduce operators' ability to monitor systems and perform control actions. It may also cause abnormal operating conditions due to erroneous automatic action or indication. Thus, from a human performance perspective, it is essential that plant personnel be able to detect the failure of a digital system and transition to backup systems when failures occur.

The U.S. Nuclear Regulatory Commission (NRC) reviews the human factors engineering (HFE) aspects of NPPs to ensure that their designs follow "state-of-the-art HFE principles" (in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 50.34(f)(2)(iii), 10 CFR 50.34(f), and 10 CFR 52.47(a)(8)). The NRC's HFE reviews help protect public health and safety by ensuring appropriate support for operator performance and reliability.

Three primary guidance documents are used to conduct HFE safety reviews. The first is NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP), Chapter 18, Revision 3, "Human Factors Engineering," issued December 2016 (NRC, 2016a). It provides high-level guidance for the conduct of HFE reviews and references two primary companion documents that give detailed review criteria. One of these documents is NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," issued November 2012 (O'Hara et al., 2012), which contains review criteria for 12 elements of an HFE program. It tracks the design process through planning, analysis, design, verification and validation, and operations (see Figure 1-5).

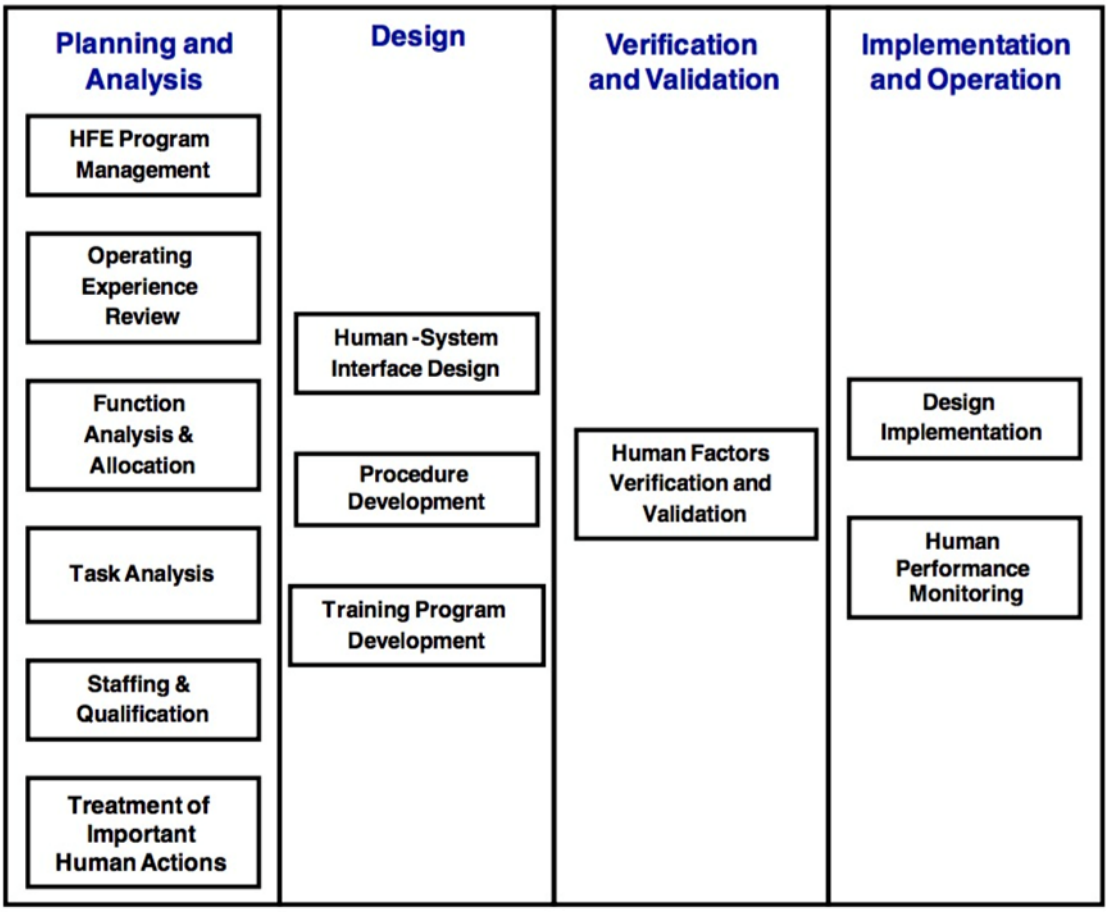


Figure 1-5 NUREG-0711 Review Elements

The other document is NUREG-0700, “Human -System Interface Design Review Guidelines” (Revision 2, O’Hara et al., 2002; Revision 3, O’Hara and Fleger, 2020). It is used to review the detailed design of the control room and other HSIs in the plant. NUREG-0700 addresses the physical and functional characteristics of HSIs. HSI design reviews are covered in the SRP and NUREG-0711.

In parallel with the HFE review in Chapter 18 of the SRP (NUREG-0800), Chapter 7, “Instrumentation and Controls,” provides guidance for review of DI&C in light water reactors. Several portions of Chapter 7 interface with the HFE review. In particular, Section 7.5 of NUREG-0800, Revision 6, “Information Systems Important to Safety,” describes the review process and acceptance criteria for those I&C systems “that provide information to the plant operators for: (1) assessing plant conditions, safety system performance and making decisions related to plant responses to abnormal events, and (2) preplanned manual operator action related to accident mitigation.” The systems reviewed include accident monitoring instrumentation, bypassed or inoperable status indication for safety systems, plant annunciator (alarm) systems, safety parameter display system, and information systems associated with the emergency response facilities and emergency response data system. These I&C systems provide inputs to the HSIs that are used by operators for controlling and maintaining safe operation of the plant. The review process and acceptance criteria in Section 7.5 of NUREG-0800 focus on compliance with four design principles: redundancy, independence, deterministic

behavior (i.e., predictability and repeatability), and diversity and defense-in-depth. In response to a need for additional guidance when reviewing DI&C applications, the NRC issued a series of Interim Staff Guidance documents associated with DI&C starting in 2007. The NRC staff have been using the methods and guidance described in these ISGs to evaluate applicant and licensee compliance with NRC requirements. Among those, ISG-DI&C-05, "Highly Integrated Control Rooms – Human Factors" (incorporated into NUREG-0800, Chapter 18, "Human Factors Engineering", Revision 3) established review criteria for digital human-system-interfaces in control rooms. ISG-DI&C-04, "Highly Integrated Control Rooms & Digital Communication Systems" (incorporated into Regulatory Guide (RG) 1.152, Rev 4), focused on licensing reviews of digital communication systems. ISG-DI&C-06, "Licensing Process," defined the licensing process for reviewing license amendment requests associated with safety-related digital I&C equipment modifications. In particular, Section D2.5 "System Interfaces" of ISG-DI&C-06 emphasizes malfunction detection of DI&C systems. The DI&C reviews interface with HFE reviews through operator actions, as illustrated in Figure 1-1.

To keep its review guidance current with industry developments, the NRC conducts research on new technology and other important issues for which review guidance is needed. I&C degradation is one such area. In view of the increasing use of digital HSI and I&C systems, the NRC staff needs guidance to evaluate the potential impact on operations when such systems degrade and fail. This report presents the technical basis and guidelines for reviewing an applicant's approach to addressing the detection and management of I&C degradation in HSIs.

1.2 Research Objectives

The objectives of this research were to (1) examine the effects of degraded HSI and DI&C conditions on human performance and plant operations, and (2) develop guidance for the review of HSI support for the detection and management of degraded HSI and DI&C conditions by plant personnel. In this study, the word "degraded" refers to a full range of conditions, from relatively minor loss of functionality to the complete failure of an HSI or DI&C system.

The scope of this research was limited as follows:

- The research focused on plant operations, even though the authors recognize that the maintenance of digital systems also plays a significant role in I&C degradation (O'Hara et al., 1996).
- The assessment was limited to typical situations in which HSI and I&C systems may degrade; it did not encompass degradation or failure due to intentional actions, such as sabotage or cyberattacks.

This report is an update of an earlier technical report (O'Hara et al., 2010), which provided preliminary design review guidance. Updates include (1) the technical basis with new information published since the earlier report, (2) the peer review of the guidance, and (3) integration of the guidance into NUREG-0700, Revision 3.

The guidance was incorporated into NUREG-0700 as a new section, Section 14, "Degraded HSI and I&C Conditions Characterization." This cross-cutting section applies to the evaluation of *all* HSIs, rather than a limited range of them, allowing reviews addressing HSI and I&C degradation to be more consistent, regardless of the type of HSI used.

1.3 Intended Use

This report is intended for the NRC staff to use in performing HFE reviews of new plant designs and of DI&C upgrades of operating plants. The report covers the methodology for developing HFE guidance; the framework for characterizing the I&C, HSI, and human operator systems; the technical basis for understanding DI&C degradation and its impacts; and HFE review guidance related to HSI and I&C degradation (in Appendix A and B). The methodology presented is not limited to the context of this report but applies to HFE review guidance development in general. The technical basis will be useful for the staff in understanding the integration of DI&C, human factors, and human reliability analysis (HRA).

1.4 Organization of the Report

This report is organized as follows:

- Section 1 is the introduction.
- Section 2 describes the methodology that the NRC uses to develop HFE review guidance.
- Section 3 presents the framework for characterizing the I&C, HSI, and human operator systems.
- Section 4 evaluates the existing literature on how HSI and I&C degradation and failure affect human performance.
- Section 5 illustrates the effects of digital feedwater system degradation on HSIs and operator performance.
- Section 6 discusses the results of the study and presents the overall conclusions, including topics for future research.
- Appendix A includes guidelines for the review of HSI designs.
- Appendix B contains guidelines for the review of the design process.
- Appendix C presents a glossary of the main concepts in this report.

2 HUMAN FACTORS ENGINEERING GUIDANCE DEVELOPMENT METHODOLOGY

The NRC has established a methodology for developing guidance on conducting HFE safety reviews (O'Hara et al., 2008a). Figure 2-1 gives an overview of the main steps in the process. A central objective of the method is to establish the validity of the individual guidelines being adopted. Validity is defined along two dimensions: internal and external. Internal validity means the degree to which the individual guidelines are linked to a clear, well-founded, and traceable technical basis. External validity means the degree to which independent peer review supports the guidelines. Peer review is an effective means of evaluating guidelines for conformance to generally accepted HFE practices and to industry-specific considerations (i.e., peer review helps ensure that the guidelines are appropriate with respect to practical operational experience of actual systems). The sections below describe each step as applied in this project.

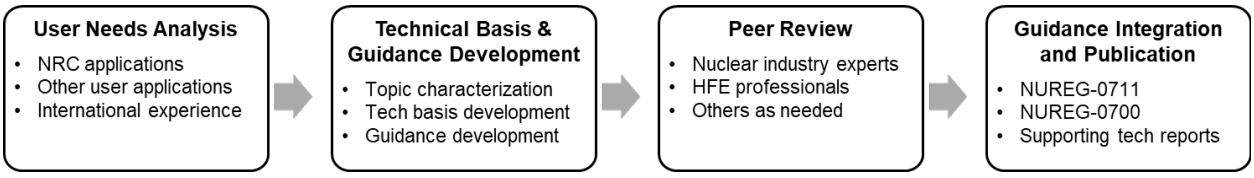


Figure 2-1 Major Steps in Development of NRC HFE Guidance

2.1 User Needs Analysis

In 2008, the NRC conducted a study to identify human performance research issues associated with the implementation of new technologies in NPPs (O'Hara et al., 2008a, 2008b). To identify the research issues, current industry developments and trends were evaluated in the areas of reactor technology, I&C technology, HSI technology, and HFE methods and tools. The study identified 64 issues. These issues were prioritized into four categories based on evaluations by 14 independent subject-matter experts representing vendors, utilities, research organizations, and regulators. Of the 64 issues, 20 were placed in the top-priority category, and among these was "operations under conditions of degraded instrumentation and controls."

As discussed in Section 1, the importance of this issue stems from the functions performed by the I&C system. The I&C system, together with plant personnel, monitors performance, takes control actions, and responds to normal and off-normal events, thus supporting safe, efficient power production. I&C degradation may significantly reduce operators' ability to monitor systems and perform control actions. It may also cause abnormal operating conditions due to erroneous automatic action or indication. Thus, from a human performance perspective, it is essential that plant personnel be able to detect the failure of an I&C system and transition to backup systems when failures occur.

The Electric Power Research Institute (EPRI) and the Nuclear Energy Institute (NEI) have also identified I&C system degradation as a crucial technical issue facing new plant development and requiring further research (Torok et al., 2006). Their report refers to the issue as "failure management for new human-system interface" and describes it as follows:

> Practical criteria and methods are needed for addressing partial or large-scale failures of the HSIs normally used by the operators. This is especially applicable to new plant control rooms, which will be more integrated and digital than

operating plant control rooms. Specific issues include appropriate operation under degraded I&C and HSI conditions, what backups should be provided, when to switch to backups, and the human factors engineering (HFE) issues associated with switching to backups, as well as integration of backups into the overall control room design.

Thus, the issue of degraded and failed HSIs and I&C systems was identified by both the NRC and industry as an important topic warranting research to better understand its effects and to provide guidance to support operators in detecting and managing the effects of I&C degradation on HSIs.

2.2 Technical Basis and Guidance Development

The second step in the guidance development process, technical basis and guidance development, consists of three phases: (1) topic characterization, (2) technical basis development, and (3) guidance development and documentation (see Figure 2-2).

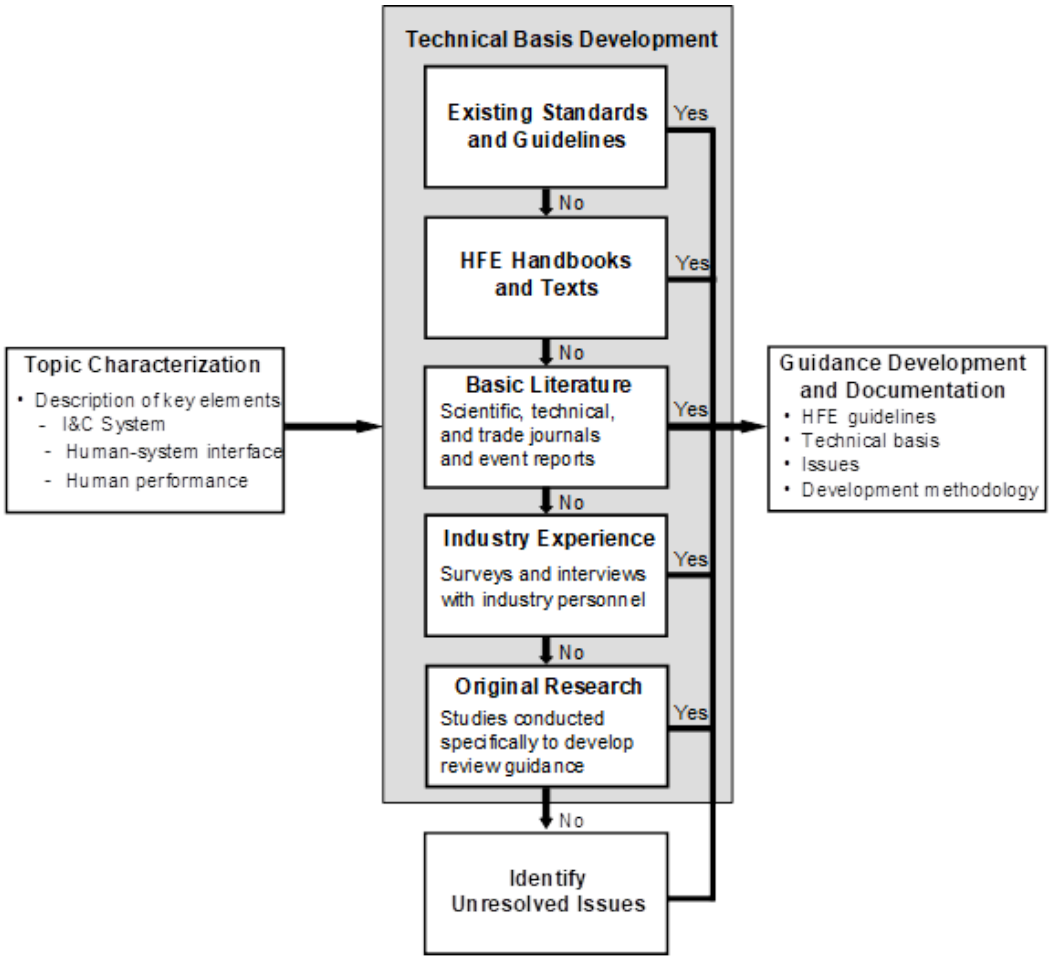


Figure 2-2 Technical Basis and Guidance Development Phases

2.2.1 Topic Characterization

For the topic characterization phase in this project, the authors developed a framework jointly characterizing DI&C systems, HSIs, and human performance. This framework describes the functional design aspects of I&C systems that are important to human performance. It was developed to be sufficiently robust to accommodate the review of the full range of I&C systems that designers may employ. The framework serves several purposes:

- It provides a way of organizing the analysis of research studies, operational events, and the like into a standardized language to support the formulation of more general insights.
- It offers a structure for developing and organizing guidance.
- It gives reviewers a structure for requesting information from applicants and licensees during a review.

In the present context, the framework makes it possible to describe how degraded I&C conditions affect operator performance. It establishes the links between the three essential levels of plant control: the I&C system, the HSIs, and human performance (see Figure 1-1). Section 3 describes this framework in detail.

2.2.2 Technical Basis Development

To develop the technical basis for the planned guidance, the authors gathered information from a variety of sources. Figure 2-2 identifies the types of sources considered, in order of preference (from top to bottom). The sources higher in the flowchart are preferable for guidance development for three reasons. First, they are already in or close to HFE guidance format, whereas the information in sources listed lower (e.g., individual research studies) must be synthesized and HFE guidelines abstracted from it. Second, the information in the sources listed higher in the flowchart has already been validated to some extent (as discussed earlier), while the information in sources listed lower needs validation before it can be used to formulate guidance. Third, the cost of obtaining information and using it to develop guidance is generally greater for sources listed lower in the flowchart.

This section provides an overview of the technical basis development process. Section 4 evaluates the existing literature on how HSI and I&C degradation and failure affect human performance. Section 5 documents an analysis of how the degradation of the digital feedwater system affects the HSIs and operator performance at an actual plant.

2.2.2.1 Evaluation of Existing Literature on Human-System Interface and Instrumentation and Control Degradation

2.2.2.1.1 Standards and Guidelines

The review of the literature began with existing HFE standards and guidelines, developed either by standards development organizations, such as the American National Standards Institute, or by other organizations, such as the U.S. military. Generally, these documents are based on research, operational experience, and subject-matter expertise. In addition, most have been peer-reviewed. They may therefore already have internal or external validity, or both. Furthermore, since they are often already in guidance form, they are generally easier to use for guidance development than other sources of information.

The authors identified several documents containing guidance on degraded I&C systems, including industry standards (e.g., from the Institute of Electrical and Electronics Engineers (IEEE)) and detailed regulations and design review guidance from the NRC. Through EPRI and the Institute of Nuclear Power Operations, the nuclear industry has established standards of performance for operations and safety in which I&C systems are a vital component. Industry organizations have also published documents (e.g., EPRI topical reports) to assist NRC licensees and license applicants with the design, licensing, and operation of DI&C systems and associated HFE considerations.

The NRC documents its analyses and regulatory positions in standard review plans, regulatory guides (RG), regulatory issue summary (RIS) reports, interim staff guidance (ISG) documents, and branch technical positions. Some regulatory guidance endorses or references industry standards. For instance, the NRC issued RIS 2002-22, “Use of EPRI/NEI Joint Task Force Report, ‘Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,’” dated November 25, 2002 (NRC, 2002), to endorse the use of EPRI TR-102348, “Guideline on Licensing Digital Upgrades” (EPRI, 2002), as guidance for designing and implementing digital upgrades to I&C systems.

Section 4.1 describes the authors’ analysis of existing HFE standards and guidelines.

2.2.2.1.2 Handbooks, Textbooks, and Basic Literature

While existing standards and guidelines provide a valuable starting point, they may not extend to all aspects of a topic. The authors therefore also consulted a range of documents analyzing and synthesizing the existing literature, including handbooks and textbooks written by experts. An example applicable to this project is the chapter “The Effects of Control Dynamics on Performance” in the *Handbook of Perception and Human Performance* (Wickens, 1986). The information in such sources is usually not presented in the form of guidance; thus, guidance must be developed from it.

For new technology, such as DI&C systems, sources such as handbooks and textbooks are often insufficient to support the establishment of guidance. In such cases, it is necessary to review basic literature, such as papers from research journals, industry conference papers, and technical reports, to derive a theoretical basis for understanding the technology.

In this project, the authors found numerous empirical studies of human-machine interactions addressing a broad range of technologies and user tasks, which could provide insight for guidance development. However, greater effort is needed to distill the information in these studies. In particular, engineering judgment must be used to evaluate whether the conclusions of specific studies can be generalized to actual applications in the workplace. The generalizability of individual experiments is limited by the unique conditions under which they were conducted, including the individual participants, the types of tasks performed, and the types of equipment used. For example, the tasks involved in laboratory experiments are often less complex than those required to operate an NPP, and they are not subject to the same performance-shaping factors (such as rotating shifts, stress, and fatigue) that exist in the nuclear industry’s work environments. While findings from basic research can be valuable in guidance development, in the context of real-world tasks and systems they must be interpreted using judgment from professional and operational experience.

Section 4.2 contains the results of the authors' analysis of handbooks, texts, and basic literature.

2.2.2.1.3 Industry Operating Experience

Information on industry experience can be obtained from reports and surveys of plant personnel, designers, and regulators—for example, through interviews, knowledge-elicitation sessions, or walkthrough exercises using an actual HSI or a high-fidelity training simulator. While this information can be difficult and costly to obtain, it is usually more directly applicable to the NPP domain than information found in basic literature. However, like information obtained from handbooks, texts, and basic literature, it needs to be critically analyzed and synthesized to be used in guidance development. For this study, the authors assessed published reports on events and operating experience pertaining to I&C degradations that affected human performance. Section 4.3 discusses the results of this analysis.

2.2.2.2 Original Research: Analysis of the Effects of Digital Feedwater System Degradation

When existing literature does not cover certain specific issues relevant to guidance development, the technical basis may be enhanced by original research. For this project, the authors examined a failure mode and effects analysis (FMEA) performed for the digital feedwater system of an operating pressurized-water reactor (PWR). They extended the analysis to determine how the degradation of the digital feedwater system could affect HSIs and operator performance. Section 5 provides the results of this analysis.

2.2.3 Guidance Development

As noted in Section 1.2, preliminary HFE review guidance was published in Brookhaven National Laboratory Technical Report No. 91047-2010, "The Effects of Degraded Digital Instrumentation and Control Systems on Human-System Interfaces and Operator Performance" (O'Hara et al., 2010). After 2010, the NRC continued to edit and supplement the technical basis as new information became available. The guidance was eventually peer reviewed and integrated into NUREG-0700, Revision 3. The updated guidance focuses on the review of (1) the HSIs used for monitoring the HSI and I&C systems and managing any degraded conditions, and (2) the applicant's design process for addressing degraded HSI and I&C conditions. Each of these topics is described below.

2.2.3.1 Human-System Interface Design Review Guidance

The updated guidance on degraded HSI and I&C conditions became Section 14 of NUREG-0700, Revision 3. The section has three parts: (1) a topic characterization, (2) a list of the review criteria used to evaluate each aspect of the HSI, and (3) a bibliography of documents giving detailed information on HSIs. The guidelines are organized into the following subsections:

- 14.1, "HSIs for Monitoring I&C System Conditions"
- 14.2, "HSI Response to I&C System Changes"
- 14.3, "Information Source and Validity"
- 14.4, "Backup of HSI and I&C Failures"

The individual guidelines are structured using the standard NUREG-0700 format, which has five elements (Figure 2-3 provides an example):

- *Guideline Number*—Within sections, individual guidelines are numbered consecutively from 1 to *n*. Each guideline's unique number consists of its section or subsection location, a dash, and then its serial number.
- *Guideline Title*—Each guideline has a unique descriptive title.
- *Review Criterion*—Each guideline contains a description of an HSI characteristic against which the reviewer may judge the HSI's acceptability. The criterion is not a requirement, and characteristics incompatible with the review criterion may be judged acceptable in accordance with the procedures in the review process.
- *Additional Information*—Many guidelines include additional information that may provide clarifications, examples, exceptions, figures, or tables. This information is intended to assist the reviewer in interpreting or applying the guideline.
- *Source*—The source document from which the guideline was developed is indicated by a superscript, which typically corresponds to a NUREG, NUREG/CR, or technical report number. In the example in Figure 2-3, the number "6633" is used, indicating that the technical basis for the guideline is NUREG/CR-6633, "Advanced Information Systems Design: Technical Basis and Human Factors Review Guidance," issued March 2000 (O'Hara et al., 2000).

14.2-2 Indication of Information Inaccuracy

Information system failures (caused by sensors, instruments, and components) should result in distinct display changes, which directly indicate that depicted information is not valid.

Additional Information: The information system should be designed so that failures in instrumentation are readily recognized by operators. When panel instruments such as meters fail or become inoperative, the failure should be apparent to the user (e.g., through off-scale indication).[6633]

Figure 2-3 Format of HFE Design Review Guideline

Appendix A to this report contains the HSI design review guidelines for degraded HSI and I&C systems.

2.2.3.2 Design Process Review Guidance

NUREG-0700, Appendix B "Design Process Guidelines," contains additional guidance on the design of selected aspects of HSIs.[1] The main sections of NUREG-0700 address the physical and functional characteristics of HSIs, not the unique design process considerations that may apply to them. For example, in the development of design review guidelines for degraded HSI and I&C conditions, training emerged as a significant factor in operators' ability to recognize degraded conditions. Appendix B captures this information. The Appendix B guidance is not a formal part of the NUREG-0700 review process, but reviewers may use it on a case-by-case

[1] This guidance differs from the more general process review guidance in NUREG-0711. NUREG-0711 does not cover design considerations for specific HSI technologies, such as alarms and controls.

basis if appropriate. Design process review guidelines for degraded HSI and I&C conditions appear in NUREG-0700, Revision 3, Section B.5.

The design process guidelines are organized and formatted like the design process guidance in NUREG-0711. They are organized into the following sections, corresponding to HFE program elements:

- B.5.1, “Operating Experience Review”
- B.5.2, “Task Analysis”
- B.5.3, “Treatment of Important Human Actions”
- B.5.4, “Human-System Interface Design”
- B.5.5, “Training Program Development”
- B.5.6, “Human Factors Verification and Validation”

As in NUREG-0711, the guidelines in each section are numbered consecutively. Each consists of a review criterion and additional information (see Figure 2-4).

(1) The applicant's task analysis should identify the task requirements for managing HFE-significant HSI and I&C degradations so that risk-important tasks can be performed.
Additional Information: Task analysis is the means by which the task requirements for managing I&C degradations are identified. Those requirements are needed to define the features of the HSI design needed to support operators in monitoring and responding to such degradations. The analysis should also include tasks associated with failure and transition to backup systems; for example, transitioning to paper procedures upon failure of a CBP system.

Figure 2-4 Format of Design Process Guidance

Appendix B to this report contains the design process review guidelines for degraded HSI and I&C conditions.

2.3 Peer Review

The third step in the guidance development process is peer review. Subject-matter experts with knowledge of HFE, I&C systems, and operations reviewed this document and evaluated its scope, comprehensiveness, technical content, technical basis, and usability. In addition, the guidance was made available for public comment. The authors revised the guidance based on the comments and suggestions of the peer reviewers and the public.

2.4 Guidance Integration and Document Publication

Before this project was carried out, Revision 2 of NUREG-0700 already contained some guidance on HSI and I&C degradation. This raised the question of whether the new guidance developed in this project would overlap or replace any of the existing guidance in NUREG-0700.

To resolve this issue, the authors evaluated each guideline in NUREG-0700, Revision 2, to determine how Revision 3 should address it. The evaluation resulted in some changes to the Section 14 guidelines, as well as to the guidelines in other sections of NUREG-0700. NUREG-0700, Revision 3, reflects all the changes.

3 CHARACTERIZATION OF THE INSTRUMENTATION AND CONTROL, HUMAN-SYSTEM INTERFACE, AND HUMAN OPERATOR SYSTEMS

This section presents the framework developed to characterize the key elements of I&C, HSI, and human operator systems, and the relationships among these elements. This characterization makes it possible to elucidate how the effects of degraded I&C and HSI conditions can propagate and impact human performance.

3.1 Instrumentation and Control System Characterization

Modern DI&C systems provide a great deal of functionality that is vital to plant performance and safety. New reactor designs use a wide range of DI&C architectures. Figure 3-1 shows a generic block diagram identifying the main components of a representative DI&C system. The blocks represent the types of digital components that are required to process a signal from the system to its end use. The arrows represent the information flows between the components. Signals from a sensor are processed through data acquisition and signal processing units and converted to appropriate formats, which might include some high-level calculated parameters. These input parameters then pass to a computerized logic unit, often containing internal software that processes the parameters and compares them to a set of criteria to decide whether a series of systems and components should be actuated. Thereafter, the signal is transmitted to actuator devices that complete the desired operation. The processed signal information is used to generate information displays in the control room. HSI displays for the operators can be fed from any of these components, although they are most commonly fed from signal processors and logic units.

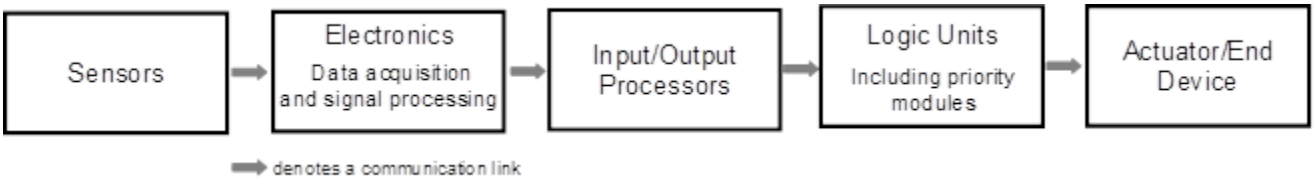


Figure 3-1 DI&C System Components

Many detailed taxonomies or classifications are available to characterize specific DI&C systems. For the purposes of this project, the authors wanted to develop an I&C characterization that would be generic, simple, high-level, and independent of the system's architecture. Such a characterization would make it possible to formulate insights that could be generalized beyond specific I&C systems. Future research can be performed to develop more fine-grained characterization schemes if warranted.

To identify a suitable means of developing a useful high-level I&C characterization, the authors reviewed several publications on the characterization of modern DI&C systems.

A limitation of a simple component characterization, such as that shown in Figure 3-1, is that it fails to address the functions of the I&C system. The I&C roadmap for the U.S. Department of Energy's (DOE's) advanced NPP programs (Dudenhoeffer et al., 2007) offers an alternative approach to representing the instrumentation, control, human-system interface (ICHSI) system (see Figure 3-2).

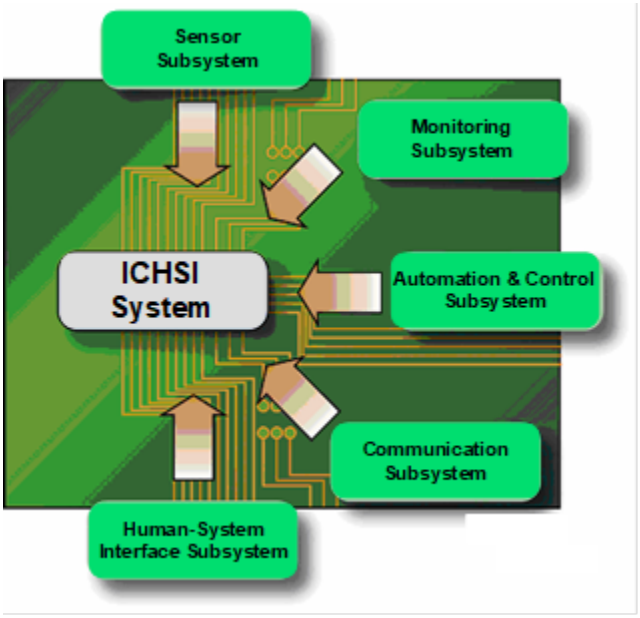


Figure 3-2 I&C Subsystem Representation Employed by the DOE for Advanced NPPs (Source: Dudenhoeffer et al., 2007)

The ICHSI system is represented by the following subsystems:

- *Sensor subsystem*—Nearly every plant process uses some form of physical measurement taken by sensors that detect plant parameters, such as neutron flux, temperatures, pressures, flow, valve positions, electrical current levels, and radiation levels. Some new nuclear energy production technologies employ novel types of sensors and instruments to measure physical processes. For example, some reactor designs include electronic sensors with embedded software that work in high-temperature environments and measure and analyze process parameters quite different from those captured in today's operating light-water reactors.

- *Monitoring subsystem*—This subsystem monitors the signals and other information produced by sensors and evaluates them to determine the appropriate response. The monitoring subsystem may perform sophisticated diagnostic and prognostic functions. Diagnostic functions serve to identify and determine the causes of deviations or faults in plant systems or processes. Prognostic functions make it possible to use sensor data to estimate the rate of physical degradation and the remaining useful life of systems, predict time to failure, and apply this information to more effectively control processes.

- *Automation and control subsystem*—Digital control systems offer the ability to implement more advanced control algorithms than those presently used in U.S. NPPs, which rely primarily on classical (single-input, single-output) control schemes to automate individual control loops. Advanced control schemes include matrix techniques for optimal control,

nonlinear control methods, fuzzy logic, neural networks, adaptive control (i.e., controls that modify their behavior based on plant dynamics), expert systems, state-based control schemes, and combinations of these methods. These advanced techniques enable more integrated control of plant systems and processes (as opposed to separate, noninteracting control loops), as well as more granular control. They may also support closer interaction and cooperation between automation and personnel, allowing plant functions to be controlled by human-and-machine teams (O'Hara and Higgins, 2010, 2017).

- *Communications subsystem*—A variety of communications systems ensure information flow throughout the I&C system and to devices being monitored and controlled. A classical I&C architecture provides point-to-point wiring of measured parameters to the monitoring and control systems. Communications subsystems for modern I&C systems are configured in a flexible network architecture and may include wireless technology. Their greatly expanded functionality enables "smart" transducers to signal their service condition to the engineering staff.

Figure 3-2 also depicts the HSI system as part of the ICHSI system. This reflects the fact that in most nuclear design organizations, the development of the HSIs falls within the overall responsibility of the I&C organization. However, given the focus of this project, this document considers the HSIs separately.

The simple generic characterization of Figure 3-2 is independent of the I&C system architecture and will serve as the framework for the rest of this document. Each subsystem identified in the framework can experience degraded conditions that could impact HSIs and operator performance. For example, Kisner et al. (2009) found that degradation of communication links can result in the same loss of information as caused by sensor failure or degradation. Communication between components and between components and personnel is a vital function throughout the plant infrastructure.

3.2 Human-System Interface Characterization

Operations personnel perform their tasks associated with I&C systems through the HSIs in the control room and local control stations. It is through the HSIs that operator actions affect plant systems and higher level plant functions, including safety functions. The HSIs thus mediate any impact that I&C degradations may have on operator performance. NUREG-0700 provides a detailed characterization of HSIs (see Figure 3-3).

The following basic elements are the building blocks of any HSI:

- *Information Displays*—The visual and auditory displays used in the main control room and at remote locations throughout the plant. Displays can be conceptualized in a top-down fashion, in terms of their function (the purpose of the information they present), their format (e.g., mimic displays or trend graphs), format elements (e.g., labels, icons, symbols, color, text, and coding), data quality and update rate, and the devices on which they appear (e.g., large flat panels).

- *User-Interface Interaction and Management*—All HSI elements related to the modes of interaction between personnel and the HSIs. These include dialogue formats

(e.g., menus, direct manipulation, and command language), navigation features, display controls, tools for entering information, system messages, and prompts. They also include methods for ensuring the integrity of data accessed through the user interface, for example, by preventing inadvertent changes in or deletion of data, minimizing data loss due to computer failure, and protecting data from unauthorized access via setpoints.

- *Controls*—HSI elements that enable operators to interact with the plant through conventional control devices, such as pushbuttons and rotary controls. Significant considerations related to controls include the system's response time and display-control integration. Note that the organizational structure in NUREG-0700 depicts soft controls as a separate system (described in Figure 3-3).

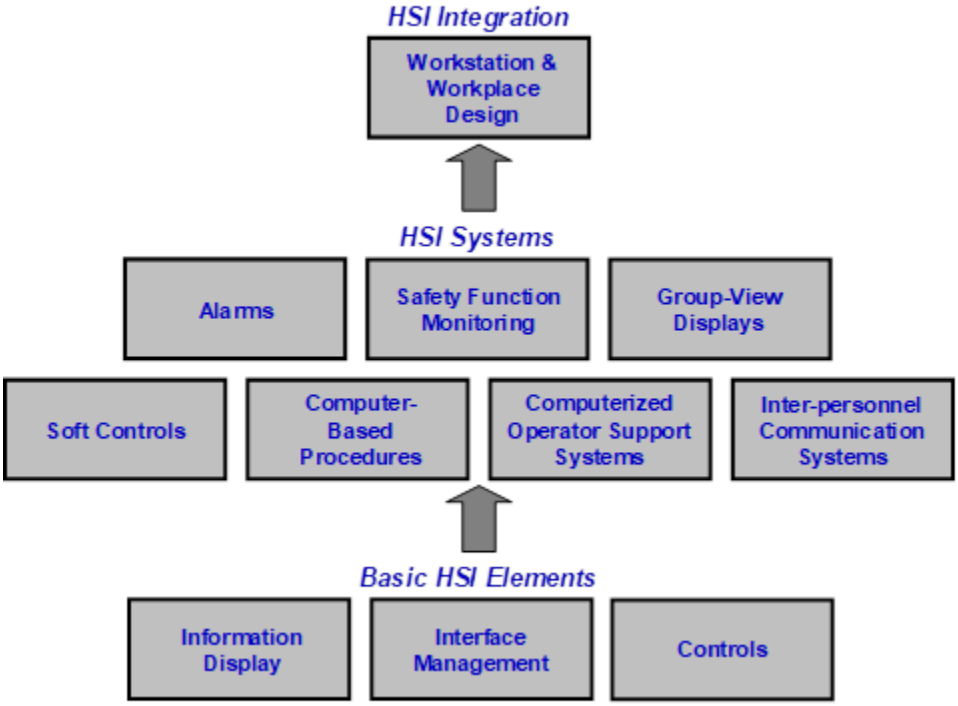


Figure 3-3 HSI Characterization from NUREG-0700, Revision 3

The three basic elements listed above constitute the building blocks of seven HSI systems, each of which performs a specific function:

- *Alarm System*—The design of the alarm system involves selecting alarm conditions, choosing setpoints, considering alarm processing and alarm availability (e.g., filtering and suppressing alarms), and the unique aspects of alarm information display (e.g., organization, coding, and alarm message content) and alarm controls (e.g., silence and reset).

- *Safety Function and Parameter Monitoring System*—This system includes the displays for monitoring critical safety functions and safety parameters.

- *Group-View Display System*—Group-view displays are those designed to be viewed from anywhere in the control room. Design considerations include their functional characteristics and user-system interaction modes, as well as their physical characteristics.

- *Soft Control System*—Soft controls are controls that are mediated by software rather than direct physical connections (e.g., onscreen control of pumps and valves). Because software mediates the control, its functions may be variable and context dependent. Also, the location of a soft control may be virtual (e.g., within the display system structure) rather than spatially dedicated.

- *Computer-Based Procedure System*—The elements of the computer-based procedure (CBP) system include the representation of procedure information, the system's functional capabilities, user interaction features, and backup resources.

- *Computerized Operator Support System*—This system assists personnel in situation analysis and decision-making. Design considerations encompass functional requirements, such as explanation and simulation facilities, and the desirable characteristics of user interfaces.

- *Interpersonnel Communication System*—This system provides the means by which plant personnel speak with each other and communicate electronically.

The HSI characterization in NUREG-0700 also includes workstations and workplaces:

- *Workstations* are the locations where HSIs are integrated to provide areas where plant personnel can perform their tasks. Workstations include consoles, panels, and sit-down desk-type configurations.

- *Workplaces* are the parts of the plant where workstations are located, such as the main control room and remote-shutdown facilities.

3.3 Human Operator System Characterization

Human operators play an essential role in the safe, efficient generation of electric power at NPPs, by monitoring and controlling plant systems to ensure their proper functioning. Test and maintenance personnel also verify that equipment is functioning properly and replace or repair malfunctioning components. While risk analyses and operating experience have established the links between human performance and plant risk, HFE principles must be applied during the design process to ensure that plant systems support effective human performance.

Operators perform many vital safety functions, and errors on their part—either errors of omission (when personnel fail to complete an action when required) or errors of commission (when personnel take the wrong action, possibly because they interpreted conditions incorrectly)—can negatively impact plant safety. Therefore, to understand how DI&C degradation could affect safety, one must examine how human errors occur and how digital technology may contribute to them. In particular, it is necessary to characterize the elements of human performance.

The authors developed the characterization of human performance described below when they first began conducting research on advanced control room technology (O'Hara, 1994). The characterization was subsequently developed further and was used as part of the technical basis for earlier HFE review guidance (O'Hara et al., 2008a).

Figure 3-4 illustrates the causal chain that mediates the impact of operators on the plant. The point at which human operators interact with plant systems occurs when personnel use HSIs to perform their tasks.

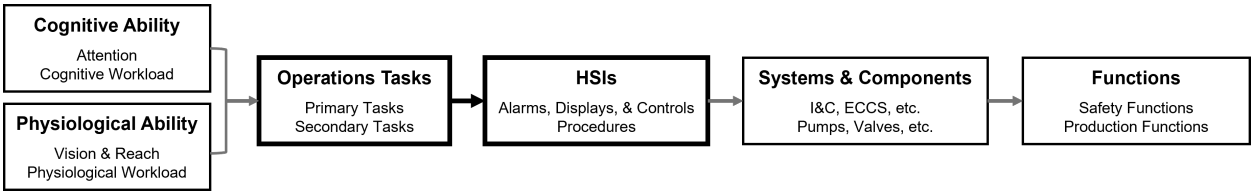


Figure 3-4 Operator Impact on Plant Safety

The operational tasks performed by personnel involve both *primary* and *secondary* tasks. Primary tasks include activities such as monitoring plant parameters, following procedures, responding to alarms, starting pumps, and aligning valves. Secondary tasks are mainly interface management tasks. Primary tasks exhibit several common cognitive elements, which can be termed *generic primary tasks*: monitoring and detection, situation assessment, response planning, and response implementation. Breakdowns in any of these tasks can lead to human error.

The first generic primary task, *monitoring and detection*, refers to the extraction of information from the environment—for example, by checking the parameters on a control panel, monitoring parameters displayed on a computer screen, obtaining verbal reports from other personnel, or sending operators to other areas of the plant to check on system components. From this information, personnel determine whether the plant is operating as expected. In a highly automated plant, much of what operators do involves monitoring. Detection is the operator's recognition that something has changed (e.g., a component is not operating correctly, or the value of a parameter has increased or decreased).

In any complex system, the task of monitoring and detection can easily become overwhelming because of the many individual functions, systems, components, and parameters involved. Therefore, an alarm system is generally used to provide support. The alarm system is one of the primary means by which abnormalities and failures come to the attention of plant personnel.

The second generic primary task, *situation assessment*, is the evaluation of current conditions to determine whether they are within acceptable limits and to identify the underlying causes of any abnormalities. As part of situation assessment, operators must actively try to construct coherent, logical explanations to account for their observations. This cognitive activity involves two related concepts: the situational model and the mental model. The latter consists of the operator's internal representation of the plant's physical and functional characteristics and its operation, as understood by the operator. The mental model is based on the operator's formal education, training, and experience. When the operator uses their mental model to interpret information about the current situation, as obtained from HSIs and other sources, the resulting

cognitive representation is termed the situation model. The term “situation awareness” refers to the understanding that personnel have of the plant’s current situation, that is, their current situation model. The alarms and displays in a plant serve to generate information supporting situation assessment. The HSIs may further support situation assessment through operator support systems, such as a disturbance analysis system.

To construct a situation model, operators use their general knowledge and understanding of the plant and its operation to interpret their observations and to extract their implications. Limitations in knowledge or in current information may lead to an incomplete or inaccurate situation model.

Situation assessment is critical to taking proper human action. An International Atomic Energy Agency (IAEA) report, Safety Series No. 75-INSAG-3, “Basic Safety Principles for Nuclear Power Plants,” (IAEA, 1988), noted this about events involving incorrect human actions:

> Frequently such events have occurred when plant personnel did not recognize the safety significance of their actions, when they violated procedures, when they were unaware of conditions of the plant, were misled by incomplete data or incorrect mindset, or did not fully understand the plant in their charge. [p. 19]

Roth et al. (1994) identified situation assessment and response planning as important factors in human performance in simulator experiments involving cognitively demanding situations (i.e., situations not fully covered by procedures or training because they occurred in conditions differing from the nominal conditions). Furthermore, in the operator reliability experiment of Beare et al. (1991), 70 percent of the crew errors in the simulator experiments were categorized as errors in situation assessment (diagnosis).

If operators have an accurate situation model but mistakenly take a wrong action, they have a good chance of detecting it when the plant does not respond as expected. However, with a poor situation model, operators may take many “wrong” actions if those actions conform to their current faulty understanding of the plant’s state.

The third generic primary task is *response planning*, which means deciding on actions to resolve the current situation. In general, it involves operators using their situation model to identify goal states and the transformations required to achieve them. There are many possible goal states, such as identifying the proper procedure, assessing the status of backup systems, or diagnosing a problem. To meet their goals, operators generate alternative response plans, evaluate them, and select the one most appropriate to the current situation model. Response planning can be as simple as selecting an alarm response, or it may involve developing a detailed plan when existing procedures prove incomplete or ineffective.

Procedures usually aid response planning. When operators can trust that suitable procedures are available to meet the current problem, the need to generate a response plan in real time is largely eliminated. However, even with good procedures, operators still need to perform some aspects of response planning. For example, in event responses, operating crews need to (1) identify goals based on their own situation assessment, (2) select the appropriate procedure(s), (3) evaluate whether the procedure-defined actions are enough to achieve those goals, and (4) adapt the procedure(s) to the situation, if necessary.

The fourth generic primary task, *response implementation*, involves performing the actions specified by response planning—for example, by selecting a control, providing control input, and monitoring the responses of the system and processes. Several types of errors are associated with the use of controls. One example is a mode error, which occurs when an operator takes an action thinking that the control system is in one mode when it is in a different one. Consequently, the system's response to the action is not what the operator intended.

Performing these generic primary tasks imposes workload. If workload is too low, vigilance suffers, diminishing the ability of personnel to perform accurate situation assessment. However, if tasks become too demanding and workload is too high, the ability of personnel to perform tasks declines.

To understand human performance, it is also important to consider secondary tasks, such as navigating or accessing information at workstations and arranging various pieces of information on the screen. These are termed secondary tasks because they are not directly associated with monitoring and controlling the plant. Personnel must successfully perform secondary tasks in order to complete their primary tasks. In part, secondary tasks are necessary because operators can view only a small amount of information at any one time through the workstation displays. Therefore, they must perform interface management to retrieve and arrange all the information needed to complete a task.

The distinction between primary and secondary tasks is important because of the ways they can interact. Secondary tasks create workload and may divert attention from primary tasks, making them difficult to complete (O'Hara and Brown, 2002). Thus, secondary tasks must be addressed carefully in design reviews. HSI and I&C degradation may increase the demands of secondary tasks; for example, when information on one display is corrupted, operators must navigate additional displays.

The discussion above focuses on the primary and secondary tasks that operators perform. However, individual operators typically do not undertake these tasks alone; they are accomplished by the coordinated activity of multiperson teams. Operators share information and work in a coordinated fashion to maintain the plant's safe operation, as well as to restore it to a safe state should a process disturbance arise. In some cases, crew members may perform a task cooperatively from one location, such as the main control room, while in other cases, a control room operator may coordinate tasks with personnel in a remote location, such as a local control station. From an HFE perspective, effective teamwork requires that all team members have common, coordinated goals; maintain shared situation awareness; and engage in open communication and cooperative planning. Successful teams monitor each other's status, back each other up, actively identify errors, and question improper procedures.

Recognition has been growing that the design of technology must consider team performance as well as individual performance (O'Hara and Roth, 2005). The transition from conventional to computer-based control rooms affects team performance in at least two ways: through changes to the physical layout and characteristics of the workplace, and through changes to the functionality of the I&C system and HSIs (such that HSIs perform activities previously performed by crew members). It is important to understand how these changes might affect both human performance and plant safety.

The effects of technology (both when it is functioning as intended and when it has degraded or failed) on human performance can be understood in terms of its effects on the factors that support human performance: primary tasks, secondary tasks, and teamwork. To the extent that technology is implemented to support these factors, it will improve human performance and therefore promote plant safety. To the extent that it is implemented in a way that undermines or disrupts these factors, it will compromise human performance and may lead to errors—which could, under the right circumstances, undermine plant safety (O'Hara et al., 2008a).

Therefore, the framework developed in this study characterizes human performance along the following dimensions:

- monitoring and detection
- situation assessment
- response planning
- response implementation
- interface management (secondary tasks)
- team processes

3.4 Framework for Characterizing Instrumentation and Control, Human-System Interface, and Human Operator Interactions

Figure 3-5 illustrates the framework developed to characterize the interactions among the I&C system, HSIs, and human performance. It consists of three levels of information flow: DI&C systems, HSIs, and human operators. The information flow between these levels is bidirectional. Each level consists of the elements described in the corresponding section above (i.e., Section 3.1, 3.2, or 3.3). The connections between the elements of different levels are open (i.e., an element in one level could potentially affect one, multiple, or all elements in the next level).

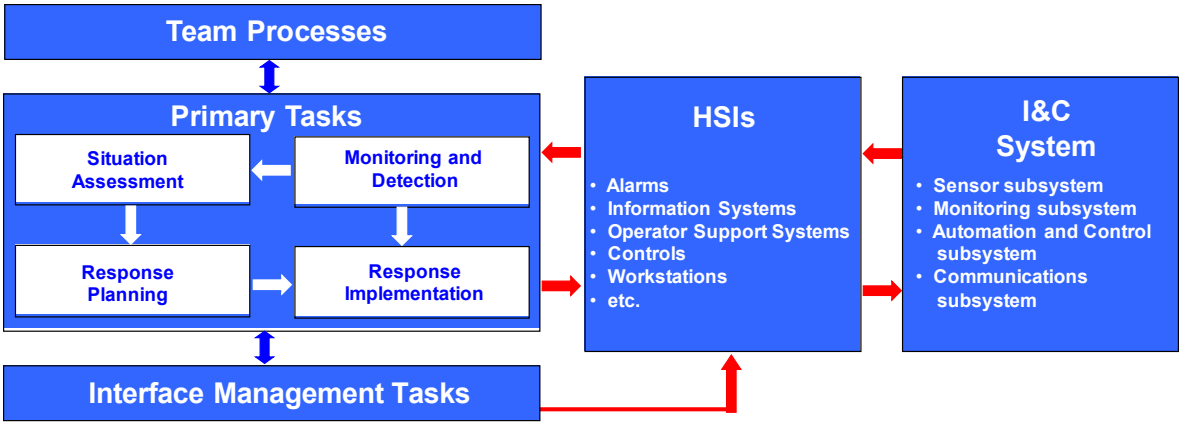


Figure 3-5 Characterization of the I&C System, HSIs, and Human Performance

The framework provides a way of organizing the information on I&C degradation gained from multiple research sources and operational events into a standardized structure from which general insights can be developed. Figure 3-6 illustrates how the framework was used in this project.

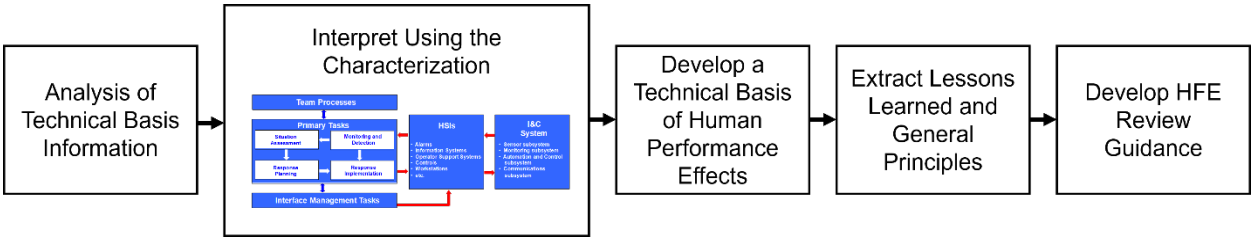


Figure 3-6 Use of the Framework in Developing Guidance

3.5 Summary

This section presents a taxonomy for analyzing the effects of I&C degradation on human performance, in order to generate insights for design. The three-level framework provides a joint characterization of I&C systems, HSIs, and operator systems, giving a clear picture of the interactions between these elements. This conceptual framework may help analysts generalize the insights from specific studies on I&C degradation to a wider range of contexts. The information in this section provides a technical basis for the development of HFE review guidance for the NRC staff.

4 EVALUATION OF LITERATURE AND OPERATIONAL EVENTS RELATED TO THE EFFECTS OF DEGRADED INSTRUMENTATION AND CONTROLS

This section presents the results of the authors' review of literature and operational events related to the effects of degraded I&C and HSIs on human performance. The material reviewed included regulatory guidelines and industry standards, handbooks, research papers, and industry operating experience.

4.1 Standards and Guidelines

The literature review began with existing standards and guidelines. Over the years, the nuclear industry has expended much effort to ensure the quality and reliability of I&C systems and HSIs used in NPPs, both by developing and implementing industry standards (e.g., IEEE standards) and by following the detailed regulations and design review guidance issued by the NRC. The NRC documents its analyses and regulatory positions in various types of regulatory and licensing documents, such as standard review plans, regulatory guides, and ISGs.

The nuclear industry also publishes supporting documents (e.g., EPRI technical reports) to assist licensees and license applicants with the design, licensing, and operation of DI&C systems, computer-based HSIs, and associated HFE.

This section summarizes the results of the authors' review of NRC and industry documents.

4.1.1 NRC Documents

4.1.1.1 Human Factors Engineering Review Criteria

This section contains a review of the following NRC-issued HFE review guidance documents:

- SRP Chapter 18, Revision 3, "Human Factors Engineering" (NRC, 2016a)
- NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model" (O'Hara et al., 2012)
- NUREG-0700, Revision 2, "Human-System Interface Design Review Guidelines" (O'Hara et al., 2002)
- DI&C-ISG-05, Revision 1, "Highly-Integrated Control Rooms—Human Factors Issues (HICR—HF)," dated November 3, 2008 (NRC, 2008b)
- BNL-91017-2010, "Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis" (O'Hara and Higgins, 2010)

SRP Chapter 18, Revision 3, "Human Factors Engineering"

The NRC addresses human performance, in part, by conducting HFE safety reviews. In accordance with 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," the NRC staff reviews the HFE programs of applicants for construction permits, operating licenses, standard design certifications, and combined operating licenses. The purpose of these reviews is to help ensure safety by verifying that the applicant's HFE program incorporates acceptable practices and guidelines, so as to appropriately support personnel

performance and reliability. SRP Chapter 18 contains high-level guidance for conducting HFE reviews (NRC, 2016a). Table 1 in SRP Chapter 18 identifies the acceptance criteria to be used for detailed HFE reviews. For most areas of HFE review related to degraded HSI and I&C conditions, the SRP cross-references the detailed review criteria in NUREG-0711 and NUREG-0700.

NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model"

The approach to HFE described in NUREG-0711, Revision 3 (O'Hara et al., 2012), rests on the concept that the HFE aspects of NPPs should be developed, designed, and evaluated based on a structured systems analysis, using accepted HFE principles. Figure 1-3 in Section 1.1 above shows the 12 elements of an HFE program review.

The elements HSI Design and Human Factors Verification and Validation address HSI and I&C degradation and failure. Section 8 of NUREG-0711 contains the review criteria for HSI design, with Section 8.4.5 specifically addressing degraded I&C and HSI conditions. The four review criteria listed below are based on a 2010 preliminary report (O'Hara et al., 2010):

(1) The applicant should identify the following:

- the effects of automation failures and degraded conditions on personnel and plant performance
- HFE-significant I&C degradations (i.e., the failure modes and degraded conditions of the I&C system that might adversely affect the HSIs personnel use to accomplish important human actions)

  Additional Information: The I&C system is made up of four subsystems: sensor, monitoring, automation and control, and communications. In this criterion, automation is considered separately due to its well-known human performance challenges and their potential impact on safety. The focus of this criterion is on HFE-significant I&C degradations. An example is a sensor degradation that results in a control room display that confuses personnel into thinking there is a process disturbance.

(2) The applicant should specify the alarms and other information personnel need to detect degraded I&C and HSI conditions in a timely manner, and to identify their extent and significance.

(3) The applicant should determine any needed back-up systems to ensure that important personnel tasks can be completed under degraded I&C and HSI conditions.

(4) The applicant should determine the necessary compensatory actions and supporting procedures to ensure that personnel effectively manage degraded I&C and HSI conditions, and the transition to back-up systems.

Degraded and failed conditions are also addressed in Section 11 of NUREG-0711. In particular, review criterion 1 in Section 11.4.1 states in part that applicants should account for I&C and HSI failures and degraded conditions, including the following:

- the I&C system, including the sensor, monitoring, automation and control, and communications subsystems; [e.g., safety-related system logic and

control unit, fault tolerant controller, local “field unit” for multiplexer (MUX) system, MUX controller, and a break in MUX line]

- common cause failure of the I&C system during a design basis accident (as defined by BTP [Branch Technical Position] 7-19)
- HSIs including loss of processing or display capabilities for alarms, displays, controls, and computer-based procedures

NUREG-0700, Revision 2, “Human-System Interface Design Review Guidelines”

NUREG-0700, Revision 2 (O’Hara et al., 2002), contains guidance for reviewing the physical and functional characteristics of HSIs. Appendix B to NUREG-0700 contains HSI-specific guidance on the HFE design process that covers the human performance problems associated with specific HSI technologies. As discussed in Section 2.4, “Guidance Integration and Document Publication,” many of the sections in NUREG-0700 have review criteria addressing degraded conditions in general.

DI&C-ISG-05, Revision 1, “Highly-Integrated Control Rooms—Human Factors Issues (HICR-HF)”

The purpose of DI&C-ISG-05 (NRC, 2008b) is to offer acceptable methods for resolving several HFE issues related to highly integrated control rooms, including the following:

- the use of computer-based procedure (CBP) systems
- the minimum inventory of alarms, controls, and displays needed
- the crediting of manual actions in diversity and defense-in-depth analyses

Degraded I&C conditions are relevant to all three of these issues. For example, the ISG states that the operator should be informed if the data presented by a CBP system have not been or cannot be validated or are invalid. In addition, the ISG states that backup systems should be available if CBP systems fail. These two aspects of design are already addressed in NUREG-0700, Revision 2, and should be part of any new guidance developed on degraded HSI and I&C systems.

The issue of crediting manual actions is also tied to that of I&C failure, specifically common-cause failure and the failure of automation functions. The ISG presents a means of demonstrating the acceptability of manual backup actions, part of which is to verify that HSIs are designed to support the credited actions. This issue is mainly covered by NUREG-0711. The NRC staff incorporated guidance from DI&C-ISG-05 for the evaluation of credited manual actions into SRP Chapter 18, Attachment A, “Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses” (NRC, 2016a).

BNL-91017-2010, “Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis”

Part 2 of BNL-91017-2010 (O’Hara and Higgins, 2010) contains review guidance on HSIs to automatic systems, including their degradation and their implications for the design process and operator training. The current report is a revised version of the BNL report. Appendix A and B of this report contain the guidelines from the BNL report that were incorporated in NUREG-0700, Revision 3.

4.1.1.2 Instrumentation and Control Review Guidance

SRP Chapter 7, Revision 7, "Instrumentation and Control"

SRP Chapter 7, Revision 7, issued August 2016 (NRC, 2016b) addresses I&C and contains two sections and an appendix that discuss, in part, degraded conditions.

Section 7.5, "Information Systems Important to Safety"

The objective of the area of review covered in SRP Section 7.5 is to confirm that the information systems vital to plant safety provide the information needed under all plant conditions. The review covers the following:

- accident monitoring instrumentation
- bypassed or inoperable status indication for safety systems
- plant annunciator (alarm) systems
- safety parameter display system
- information systems associated with the emergency response facilities
- emergency response data system

Section 7.5 provides guidance on the need to give operators timely information and status reports on the DI&C system, so they can mitigate the effects of unexpected system unavailability. While this guidance is intended to support operator awareness, it does not directly impact the current guidance development effort.

Section 7.7, "Control Systems"

SRP Section 7.7 states the following:

> The control systems covered by this SRP section include those control systems that control plant processes having a significant impact on plant safety. These control systems are those systems that can, through normal operation, system failure or inadvertent operation, affect the performance of critical safety functions.

SRP Section 7.7 states that analyses of design-basis accidents should account for the impact of failures of the control system. HSI designers should use the results of these analyses in determining how information will be communicated to operators.

Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems"

Appendix 7.0-A gives an overview of the process for reviewing DI&C systems. It notes, "Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior." The guidance in Appendix 7.0-A is not directly related to the current guidance development effort. However, it is essential that operators be aware of the potential for unexpected behavior and the need to have plans for responding to it. The guidance in the current document is intended to support such operator awareness.

4.1.1.3 Other Review Criteria

SRP Chapter 8, Branch Technical Position 8.5, Revision 3, "Supplemental Guidance for Bypass and Inoperable Status Indication for Engineered Safety Features Systems"

Branch Technical Position 8.5, Revision 3, issued March 2007 (NRC, 2007c), is part of SRP Chapter 8, "Electric Power" (NRC, 2014). It supplements Regulatory Guide 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," issued February 2010 (NRC, 2010), providing additional guidance on the design of the bypassed and inoperable status indication systems for engineered safety features. Position 6 in Branch Technical Position 8.5 states, "The indication system should include a capability of assuring its operable status during normal plant operation to the extent that the indicating and annunciating function can be verified." This position highlights the need to inform the operator of degraded or failed system status.

DI&C-ISG-03, "Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments"

DI&C-ISG-03, dated August 11, 2008 (NRC, 2008c), offers interim guidance on the evaluation of DI&C system probabilistic risk assessments (PRAs), including the analysis of common-cause failures and uncertainty associated with DI&C systems. It notes that the combination of hardware and software found in a DI&C system "can result in the presence of faults and failure modes unique to DI&C systems." Appendix B in this document addresses the treatment of I&C failures in PRA. The NRC staff incorporated the guidance in DI&C-ISG-03 into Revision 3 of Section 19.0 of NUREG-0800 (NRC, 2015).

DI&C-ISG-04, Revision 1, "Highly-Integrated Control Rooms—Communications Issues (HICRc)"

DI&C-ISG-04, Revision 1, dated March 6, 2009 (NRC, 2009a), describes how to combine controls and indications into a single integrated workstation while maintaining separation, isolation, and independence. With respect to failures of the communication system, the principal focus of the ISG is on how the overall system responds to failures. It also addresses the use of safety-related and non-safety-related controls and displays at workstations.

The ISG states that "failure of the [communication] system to meet the limiting cycle time should be detected and alarmed." Appendix A, Section A.3, of this document addresses the alarming of the I&C system.

Section 3.2 of the ISG, which addresses human factors considerations, states the following:

> … an applicant would need to demonstrate that Human Factors considerations, including consideration of operator response time and situation awareness, are consistent with the system design bases, operating procedures, and accident analyses and are both reasonable and adequate given the possibility of erroneous or inaccurate indications from the nonsafety equipment. In the context of the failure of nonsafety control stations, situational awareness involves the operator's ability to identify erroneous operation of equipment or indications, and take the appropriate actions. [pp. 14–15]

NUREG-0711, Section 11.4.3, "Integrated System Validation," addresses this general guidance in its discussion of the validation of crew performance in the face of I&C failures. Section B.5.6

of Appendix B to NUREG-0711 also addresses this topic. The NRC staff incorporated the guidance from DI&C-ISG-04 into Revision 4 of RG 1.152 (NRC, 2023).

Regulatory Guide 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"

Regulatory Guide 1.47, Revision 1 (NRC, 2010), describes an acceptable way of increasing the operator's knowledge of plant status by supplementing administrative procedures with automatic indications of the bypass or inoperability of each redundant portion of a system that performs a safety function.

NUREG-0711, Section 8.4.4.2, "Main Control Room," Criterion 2, "Bypassed and Inoperable Status Indication," contains guidance on the HFE aspects of bypassed or inoperable status indicators.

Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.152, Revision 3, issued July 2011 (NRC, 2011), describes a method for promoting the functional reliability of computers used in safety systems. It states that the system should ensure that displays do not present "erroneous plant status information to the operators." The new guidance in Appendix A, Section A.3, of this document addresses the display of erroneous information.

4.1.2 Industry Documents

The IEEE and EPRI have developed many standards and technical reports on digital HSI and I&C systems. This section summarizes the documents that address the failure or degradation of these systems.

IEEE Standard 1023-2004, "IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities"

IEEE Standard 1023-2004 (IEEE, 2004) provides recommended practices to integrate HFE into the design, operations, and maintenance of NPPs. Section 5.3.5, "Reliability and Failure," provides guidance on dealing with failures in general, not necessarily I&C or HSI failures. The guidance emphasizes the need to support operator recognition of, and response to, failures. It states that designers should address the following:

- how users can determine when a system or piece of equipment has malfunctioned
- how users should respond when such a malfunction is indicated

It also emphasizes the need for operator training to support these functions.

EPRI TR-102348, "Guideline on Licensing Digital Upgrades"

EPRI TR-102348[2] (EPRI, 2002) was written "to help nuclear plant operators implement and license digital upgrades in a consistent, comprehensive, and predictable manner." EPRI TR-102348 defines "failure management" as the ability to identify failures and to alarm them, stating that "good failure management will result if the design includes consideration of plausible failures and defects and provides appropriate features to detect the results of such events." The NRC endorsed EPRI TR-102348 in RIS 2002-22 (NRC, 2002). The NRC staff's position is that since there are no established consensus methods for accurately quantifying the reliability and dependability of digital equipment, applicants should perform a failure analysis with an appropriate level of detail to properly assess the potential for and impact of failures. EPRI TR-102348 covers human factors issues associated with replacing DI&C systems and offers the relevant guidance.

EPRI TR-1008122, "Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification"

EPRI TR-1008122 (EPRI, 2004) contains extensive guidance on the modernization of control rooms using digital HSI and I&C technology. It addresses the analysis of degraded HSI and I&C conditions and the design of HSIs to support operators' situation awareness and management of such conditions. Three sections discuss the analysis of degraded HSI and I&C conditions: Section 2, "Control Room Modernization Planning"; Section 5, "Regulatory and Licensing Activities," and Section 6, "Special Topics Related to Operations and Maintenance."

Section 2 of EPRI TR-1008122 states that the concept of operations for a plant design should explicitly account for operations under degraded HSI and I&C conditions. Guideline 4 in Table 2-8, "Guidelines for HSI Migration," states, "Ensure that potential failure modes and degraded conditions of the I&C and HSI are appropriately addressed in the design, training, procedures, and Concept of Operations as each step change is made."

Furthermore, the report states that analyses should be conducted to determine the potential impact of degraded conditions on operators. These analyses may be challenging, since digital systems introduce numerous failure modes with "sometimes subtle and wide-ranging effects." Determining these effects requires significant input from operations personnel.

Specific engineering evaluations that may have HFE-related elements include the following:

- HFE evaluations
- system failure analysis
- diversity and defense-in-depth analyses
- digital system dependability evaluation
- evaluation of modern solutions for safety monitoring and control
- evaluation of risk and other interactions with the PRA

[2] This document was also published as NEI 01-01, "Guideline on Licensing Digital Upgrades," issued March 2002.

For changes that impact the control room and other HSIs, the failure analysis should consider both HSI failures and potential human errors in using the HSI (including both operator and maintainer errors). The failure analysis should address the following:

- the impact of I&C failures on operations (considering different failure modes, inaccurate indications to the operators, potential for confusion about failures, and the treatment of I&C failures in training)
- whether failure scenarios have been tested or validated
- the impact of HSI failures (considering loss of data to update displays, loss of alarms, display failure, and loss of entire workstations, including control capability)
- the management of I&C and HSI "pre-failure" situations, where problems have been detected (e.g., through self-diagnostics) but the system is still functional

Any identified failures with new results (not previously analyzed) should undergo an evaluation in accordance with 10 CFR 50.59, "Changes, tests and experiments."

Section 6.4.3.5, "Design for Conditions in Which HSIs Are Failed or Degraded," of EPRI TR-1008122 further discusses the results of failure analyses, in terms of the need to incorporate diverse HSI capabilities to address situations in which the HSIs normally used are lost or degraded. The extent of the diverse HSI capability needed depends on how the concept of operations addresses the loss of the normal HSIs. Possible responses include the following:

- Immediately shut down the plant.
- Maintain the current state for a specified period (assuming the reactor is at power and no secondary event has occurred) and monitor plant safety functions for the need to shut down.
- Support power maneuvers.
- Handle plant upsets and emergencies.

Backup HSIs can be implemented using either conventional or computer-based equipment, provided that the equipment is not subject to the same failures as the systems it is intended to back up.

Section 4, "HFE Guidelines," of EPRI TR-1008122 addresses the design of HSIs to communicate information about degraded conditions to operators. Section 4.1.7 addresses data quality; it includes guidelines on data validation and on providing indication to the operators when data are invalid or when their validation status is unknown (e.g., when redundant sensors are not available).

The guidance states that display features should indicate to the user that the system is operating properly or that a system failure has occurred. For example, failures due to sensors should result in distinct display changes that directly indicate that depicted plant conditions are invalid.

EPRI TR-3002011816, "Digital Engineering Guide: Decision Making Using Systems Engineering"

EPRI TR-3002011816 (EPRI 2021a) provides a holistic systems engineering process to diagnose and balance all safety considerations through each phase of design. The process

starts with hazard analysis (via HAZCADS; see below) to identify potential risk areas, including I&C degradations, and incorporates the Human Factors Assessment Methodology, which provides a graded approach to human factors analysis. Section 3.4.2 provides high-level guidance on identifying and analyzing the potential consequences of errors. Here the word "error" means a mistake in the outcome of an activity, a malfunction caused by an I&C system or component, or a malfunction caused by a human error. Errors are viewed in the broad context of the risk associated with making a facility change. A high-consequence error is defined as one in which the I&C system or component has the potential to directly cause any of the following:

- reactor scram/trip
- significant reactor or plant electrical power transient of more than 20 percent rated power
- a component failure in a front-line system needed for maintaining reactor coolant
- inventory following a loss-of-coolant accident
- loss of a highly safety-significant or risk-significant function
- complete loss of a critical safety function: core cooling; reactor coolant system or spent fuel pool heat removal; containment isolation; temperature, pressure, or reactivity control; or vital alternating current electrical power

If an I&C system or component is determined to be of high consequence, then relevant downstream activities, including human factors and HRA, should be performed rigorously to manage the risk originating from potential DI&C errors.

EPRI TR-3002016698, Revision 1, "HAZCADS: Hazards and Consequences Analysis for Digital Systems"

HAZCADS provides a practical, risk-informed engineering method to determine an appropriate level of control method effectiveness, commensurate with risk, for each element of a DI&C system (EPRI, 2021b). It uses systems-theoretic process analysis (STPA) and fault tree analysis (FTA) to identify system hazards and associated unsafe control actions. FTA and risk matrices are used to formulate risk reduction targets. STPA is effective in identifying potential control system errors in digital systems, and FTA is effective in identifying random hardware failures in digital systems and their sensitivity relative to top events. The risk reduction target developed from HAZCADS provides input for other processes governed by EPRI's Digital Engineering Guide (EPRI TR-3002011816), such as digital reliability analysis and human factors analysis to mitigate or eliminate risks.

4.1.3 Summary

Existing standards and guidelines and related documents addressing HSI and I&C degradation emphasize the importance of conducting analyses to examine the effects of degraded conditions, designing HSIs to help operators to recognize and manage degraded conditions, and providing training to help operators respond properly to degraded conditions.

4.2 Analysis of Handbooks and Research Literature

As illustrated in Figure 2-2, the next sources of information consulted for this study were HFE textbooks and basic research literature on HSI and I&C degradation. This section describes the literature reviewed. Few studies examine the effects of HSI and I&C degradation on human

performance, although many focus specifically on the degradation of sensors and monitoring subsystems; for these, refer to Section 4.2.1.

Section 4.2.2 covers the research on automation, which is relevant to the degradation of the automation/control subsystem, and on time delays, which offers clues about the degradation of the communication system. The literature also addresses methods and design features to minimize the effects of such degradation.

4.2.1 Degraded Sensor and Monitoring Subsystems

The Halden Reactor Project conducted a study of two NPP crews, examining how they managed degraded monitoring conditions during accident scenarios (Kaarstad and Nystad, 2019; Nystad et al., 2019). The PWR simulator at the Halden Man-Machine Laboratory was used. The study focused on how the crews detected the degraded conditions and whether they could develop an accurate situation model of the resulting plant conditions. Five scenarios were used: a baseline scenario with no instrument failures, and four scenarios with either missing or incorrect indications. Of the latter, two scenarios involved a medium level of degradation, and the other two involved a high level of degradation. The degradation occurred during accidents such as steam generator tube rupture. Each crew experienced each of the five scenarios. Dependent measures included questionnaire ratings of scenario complexity, crew performance, and post-experiment interviews. The researchers also assessed operator trust in the HSIs. Since only two crews were used, the analysis was qualitative.

The results indicated that the crews successfully detected the degraded conditions in most but not all the scenarios. When degraded conditions went undetected, the crew was focused either on other aspects of the accident conditions not dependent on the failed indicators or on the details of the current procedures. When degradation was detected, it was typically because a suspect indication was brought to the attention of the entire crew, upon which the crew used other indicators to test its validity. In some cases, the crew performed an operation, such as opening a valve, that should have caused an indication to change in a known way, and the indication failed to change as expected. In most cases, the overall effects of the degradation were to create initial confusion and to increase the time required to manage the scenario. The crews had difficulty constructing an overview of the accident if they did not detect the degradation. When they did detect the degradation, they needed additional time to identify the problem. Instrumentation failures also led crews to use incorrect procedures. Operators reported less trust in the HSIs when they presented incorrect information than when information was missing.

Several other studies have been performed to examine the effects of sensor degradations on graphical HSIs and human performance. Vicente and Rasmussen (1992) identified sensor noise[3] as one potential limitation to implementing graphical user interfaces and called for empirical research on the issue. This led to a series of studies examining this issue.

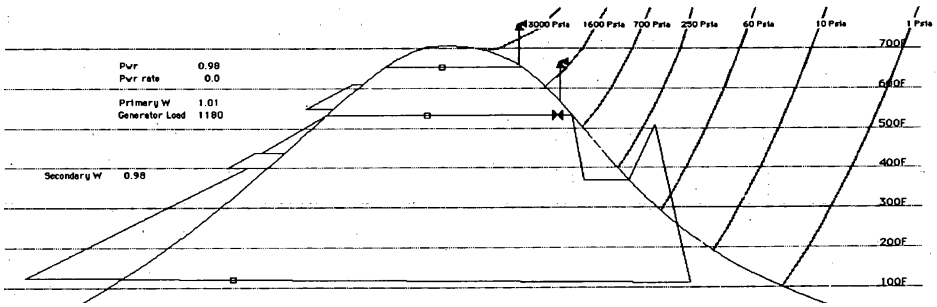
Moray and his colleagues (Moray et al., 1993, 1994; Vicente et al., 1996) undertook a study for the NRC comparing the performance of crews using a graphic display with that of crews using two types of “traditional” displays. The graphic display was a configural display, with inputs from 35 sensors, based on a plant’s Rankine cycle;[4] it was referred to as a direct perception interface

---

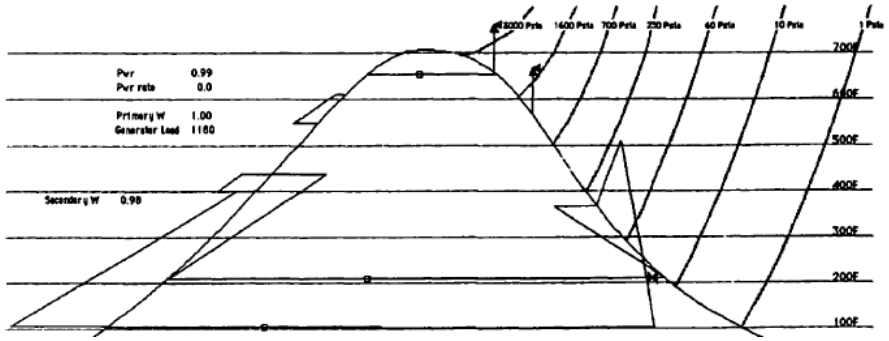
[3] Noise is irrelevant data that hampers the recognition and interpretation of data of interest.

[4] O’Hara et al. (2002) give a detailed explanation of the Rankine cycle display.

(DPI). The emergent feature was a curve connecting sensor values (see Figure 4-1). The two traditional displays were (1) analog linear gauges, and (2) analog linear gauges with a pressure-temperature plot.



Display of Normal Conditions



Display Resulting from a Failed Sensor

Figure 4-1 Effect of Failed Sensor on DPI (Source: Moray et al., 1993)

Three groups participated in the study: novices (upper-class undergraduates), experts (graduate students), and professional NPP operators. Nine transient scenarios, such as a loss-of-coolant accident, were presented on a desktop computer. No actual simulation was used during the study, but the displays were based on data collected during actual simulation trials with a simplified PWR model. Two of the scenarios presented were (1) a failed instrument (steam generator pressure failed to zero) and (2) a drifting instrument (steam generator level drifted from normal to zero). Measures of performance were the quantitative recall of parameter values, the qualitative recall of plant states, fault detection, and fault diagnosis.

Overall, the study suggested that the use of the DPI improved each group's detection and diagnostic performance. Unfortunately, in their data analysis, the authors did not address the specific effects of sensor failures on performance. However, they noted that these failures affected the participants' behavior and their understanding of the display. Moray et al. (1994) observed that when only 1 of the 35 instrument sensors failed, the display was very difficult to interpret (see Figure 4-1, which illustrates the considerable deviation that can be caused by the failure of a single sensor).

Moray et al. (1994) commented as follows:

> …the failed sensor makes the geometry of the Rankine cycle display become physically meaningless, and leads to a display which is extremely hard to interpret, although only a single variable is faulty. In this situation the loss of a single variable in the analog display left 34 variables displayed in a way which allowed them to be used for assessing plant state, but the DPI collapsed into a format which would have been extremely difficult to use, even though the plant state was in fact normal.
>
> The calculations involved in coupling information from many sources to produce the DPIs are extremely vulnerable to certain classes of failures. Little or no research exists in this aspect of DPIs, and is urgently needed. The real advantages of such displays during normal operation and during many classes of transients may be more than offset if they collapse under other classes of abnormalities.
>
> An understanding of the failure modes of DPIs (as distinct from the failure modes of the plant itself) is as necessary as an understanding of their design for normal conditions. Existence proofs of interface designs are no substitute for full empirical evaluations, and yet very few advanced DPIs have been exhaustively evaluated over a wide range of abnormal conditions. It is clear from our results that DPIs and/or ecological interfaces can fail in catastrophic ways, and it is probable that such failures may be particularly dangerous in large richly coupled systems. [p. 485]

Vicente et al. (1996) commented that it is essential to evaluate displays under these types of failure modes to ensure that they are comprehensible and do not mislead operators about what kind of process failure has occurred. Furthermore, Vicente (2002) identified sensor noise and failure as an unaddressed and potentially worrisome challenge in the use of graphic displays. He indicated the need for work to resolve this high-priority issue.

Reising and Sanderson (2000, 2004) sought to quantitatively assess the ability of operators to distinguish sensor failures from process failures. In their experiment, four groups of college students performed a process-control task using a simple pasteurizer simulation, Pasteurizer II (an interactive microworld depiction of a pasteurization process). To monitor and control the process, participants used either an ecological interface design (EID) display[5] or a piping and instrumentation display (PID). Information in the displays was supplied by either a maximum sensor configuration or a minimum one. The following example, adapted from Reising and Sanderson (2002a), illustrates the concept of each sensor configuration. Figure 4-2 presents a display portion of a simple reservoir system consisting of a tank with an input pipe and an output pipe. The display portion gives the operator information about the value of each of these three parameters. The information can be obtained for three sensors, one for each parameter (a level transmitter in the tank, and flow transmitters in the input and output pipes), which is the maximum sensor configuration. Alternatively, the information can be obtained from only two

---

[5] EID refers to an approach to display design that focuses on presenting information at various levels of abstraction, from low-level parameter information about a component to the status of high-level plant functions, such as critical safety functions. EID principles are centered on maximizing the value of an information display by using fully graphical features. O'Hara et al. (2000) give more information.

sensors (e.g., sensors for the tank level and the flow out, so that the value of *flow in* is calculated from the other two, that is, from the rate of change in tank level). *Flow in* is needed to display the emergent feature (the line connecting *flow in* and *flow out*, which indicates the rate of change) commonly used in EID displays.[6]

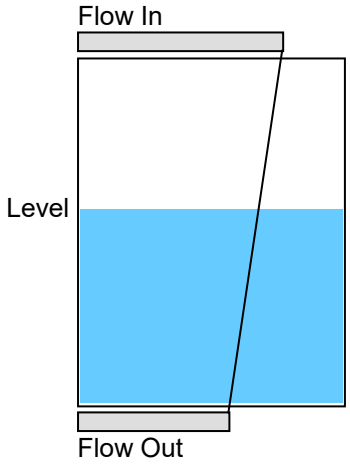


Figure 4-2 Display Showing the Tank Level, Flow In, and Flow Out

The participants in the experiment were divided into four groups of 11 individuals, each group working with one of the two display types and one of the two sensor configurations. Either process or sensor failures were introduced during selected trials. The dependent measure was the group's diagnosis of the fault. A significant crossover interaction was observed: performance was best for the EID display with the maximum sensor configuration and worst for the EID display with the minimum sensor configuration, while performance in the two conditions with the PID fell in between. However, correct diagnoses were below 50 percent in all but the EID display with the maximum sensor configuration. These results indicate that participants had difficulty distinguishing between failures of processes and failures of sensors. Performance improved under the maximum sensor configuration, which provided the most opportunities for comparison of related performance parameters. Furthermore, the sensor configuration affected the EID display more strongly than the PID; thus, diagnostic performance was worse with the minimal sensor configuration, for the reason discussed below.

To illustrate the advantages of the maximum sensor configuration, consider the displays in Figure 4-3. The upper and lower sets of displays respectively represent the minimum and maximum sensor configurations (as defined above, with the minimum configuration comprising sensors only for the tank level and the flow out). Each set shows the display at three time points after a sensor failure (which occurs at Time 1); namely, the level transmitter is degraded and drifts upward.

---

[6] NUREG-0700 defines an "emergent feature" as a high-level, global perceptual feature produced by the interactions among individual parts or graphical elements of a display (e.g., lines, contours, and shapes) to convey the relationships between them.

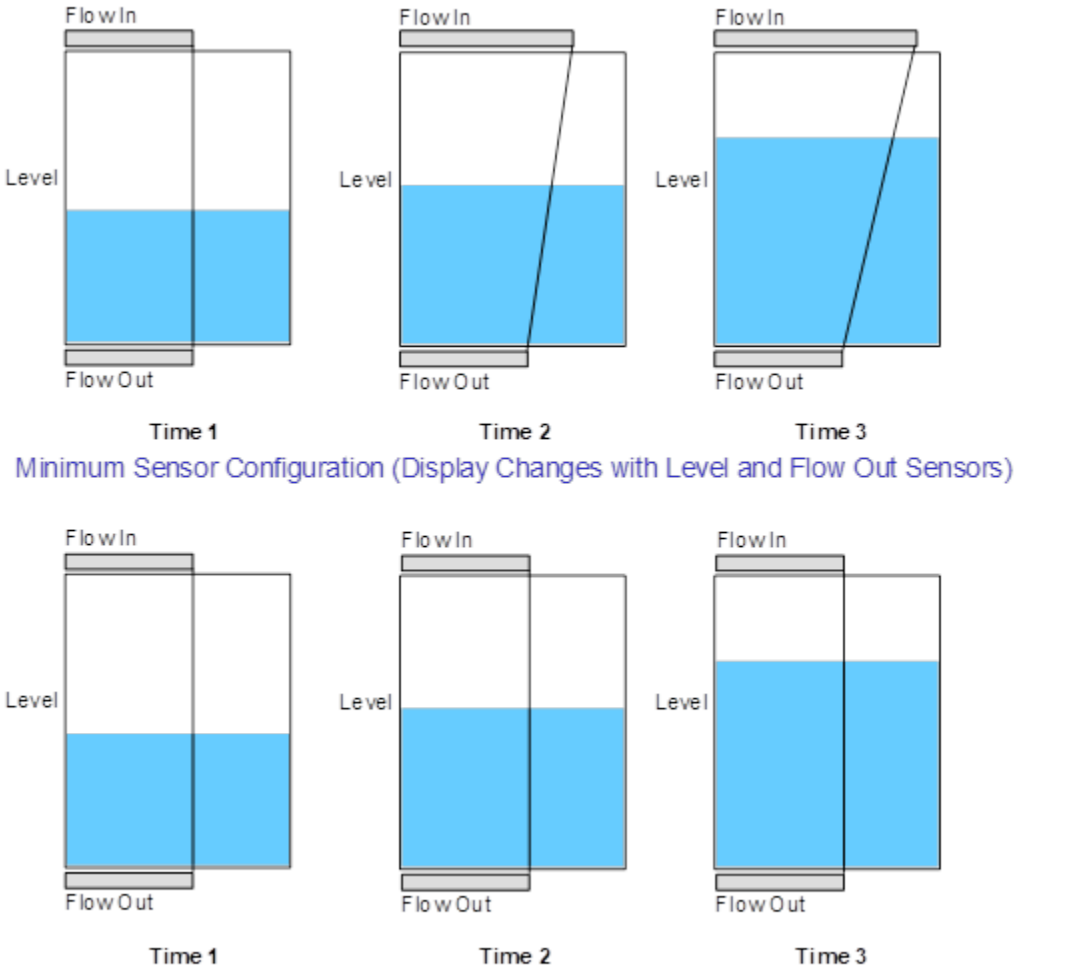


Figure 4-3 Effect of Sensor Configuration on Display (Adapted from Reising and Sanderson, 2002a)

With the minimum sensor configuration (upper set of displays in Figure 4-3), after the level transmitter fails, the display depicts an increase in tank level *and* a corresponding increase in flow in (which is derived from tank level) relative to flow out. These readings will make sense to an operator: they indicate that the tank level is increasing because more fluid is flowing into the tank than out of it. Consequently, the display is ambiguous: it does not allow operators to distinguish a sensor failure from an actual change in level. Since operators are taught to "trust their instrumentation," it is unlikely that an operator viewing this display will consider that a sensor failure may have occurred.

With the maximum sensor configuration (lower set of displays in Figure 4-3), after the level transmitter fails, the display shows the tank level as rising; however, *flow in* and *flow out* are the same. Thus, the operator can see that something is wrong: sensor degradation is likely.

This example also shows that improved instrumentation can sometimes help operators distinguish between sensor issues and process disturbances. Reising and Sanderson (2002b) give additional examples illustrating this point.

St-Cyr and Vicente extended the work of Reising and Sanderson, specifically examining the effects of sensor noise on the performance of an operator controlling a simulated thermal-hydraulic process (St-Cyr and Vicente, 2004; St-Cyr and Vicente, 2005; St-Cyr, 2006). Their first study (St-Cyr and Vicente, 2004) examined how the magnitude of sensor noise affected the performance and control strategies of 20 engineering undergraduate students. This experiment used DURESS II (Dual Reservoir System Simulation), a dynamic simulation of a simple thermal-hydraulic process. The process consists of two redundant feedwater streams that feed two reservoirs under various configurations, with time lags on control variables. The operators try to keep each reservoir at a specific temperature and to maintain water levels as needed, based on flow rates. They accomplish this task by controlling valves, pumps, and heaters. The equipment may be damaged if it is operated improperly—for example, if the water level in a reservoir is allowed to get too low while the reservoir is being heated.

Participants controlled the simulation using one of two interfaces: a basic physical representation of the process (P interface), and a physical plus a functional display (P+F interface). The P interface was a mimic-type display showing information about the two feedwater systems. The P+F display contained the same information along with information about system functions displayed using emergent features like the rate-of-change line in Figure 4-3.

The magnitude of sensor noise used in the study was based on industrial standards (by averaging accuracy ranges for sensors from different vendors). The magnitude of noise was varied randomly across trials.

Performance measures included (1) trial completion time (TCT) (i.e., the time needed to achieve a steady-state condition), (2) control stability, measured in terms of the number of oscillations around four goal variables, and (3) control recipes (i.e., instructions prepared by each participant to describe how the steady state was achieved).

The performance of participants in both groups worsened as the magnitude of sensor noise increased (i.e., TCT increased and control stability decreased). Noise also caused participants to change their control strategies, although the effect was more pronounced in the P+F group. The authors attributed this effect to the fact that emergent features were less helpful as sensor noise increased, forcing changes in strategy.

Because the magnitude of sensor noise was randomly varied, the researchers could not determine the effects of specific levels of noise. The authors explored the latter in a second study (St-Cyr and Vicente, 2005), again employing the DURESS II simulation, two interface types, and the TCT and oscillation measures. Twenty students performed the simulated task for 110 trials. The “industry standard” noise was applied to all sensors for the first 60 trials. Then, over the next 50 trials, the noise was increased by scaling multipliers of 2 (trials 61–70), 3 (trials 71–80), 5 (trials 81–90), 7 (trials 91–100), and 10 (trials 101–110).

As sensor noise increased, TCT increased (performance worsened). The effect was greater for the P+F interface. While this finding was consistent with the results of the first study, the findings in relation to the oscillation measure differed. In terms of the oscillation measure, the performance of the participants using the P interface did not worsen consistently as noise increased. Rather, it declined at first, then (at the two higher noise levels) returned to a level equivalent to that observed under the industrial average noise. The authors hypothesized that this effect might reflect a shift in control strategy, but this could not be verified (information about control strategies was not obtained). Overall, the results of this study are consistent with those

of the previous study: sensor noise impairs performance, and the effect generally is worse for those using the P+F interface.

In these two studies, changes in sensor noise were applied globally to all DURESS sensors. This is not representative of what is likely to happen in an actual system, where only one or a few sensors would be faulty at any one time. A third study addressed this scenario (St-Cyr, 2006). Again, 20 students participated, and the same DURESS II simulation, interface types, and performance measures were used (i.e., TCT, control stability (oscillations), and reported control strategies). The magnitude of sensor noise was increased on selected sensors to 10 levels above the industrial average. In this experiment, the introduction of noise did not affect the TCT and oscillation measures of the P group but worsened those of the P+F group. The analysis of control strategies revealed that while participants in the P+F group used the emergent features as a focal point of control when noise was low, they changed their control strategy as noise increased, since the noise distorted the emergent features they had been relying on. The P group was unaffected because it did not have the graphic features to influence its behavior. In summary, the studies reviewed above yield the following lessons:

- Sensor degradation can make displays difficult to understand.
- The performance of operators using graphical displays, especially displays employing emergent features, is more strongly affected by sensor degradation than the performance of operators using more traditional displays.[7]
- Operators may have difficulty distinguishing between process and sensor failures.
- Improved instrumentation can help operators distinguish between process and sensor failures by supporting comparisons of related performance parameters.
- Operators' task performance worsens as the magnitude of sensor noise increases.
- Operators change their control strategies as sensor noise rises, particularly when using EID displays. This behavior may compensate for a decrease in the usefulness of emergent display features as noise increases.

These studies show that sensor degradation can affect displays and human behavior in complex ways. Two further examples illustrate this point. First, suppose an operator is monitoring a plant in a steady-state condition, such as at 100 percent power, under relatively unchanging plant parameters. Then the HSI shows a drop in the pressurizer level. This may lead the operator to suspect a problem is developing, when in fact a degraded sensor is giving false level readings. Second, suppose an operator takes a control action to increase the pressurizer level and observes the HSIs to make sure the level is increasing. If no change is observed, the operator may conclude that a pump or valve has failed, when in fact the level sensor is degraded—that is, the level is increasing, but the HSI does not show the increase. Figure 4-4 illustrates the complex relationship between various possible sensor conditions and an operator's situation assessment.

---

[7] This finding might suggest that graphical displays should be avoided. However, considerable research has demonstrated the effectiveness of such displays in supporting operator performance, especially during unplanned and unanticipated events (Burns et al., 2008; Jamieson et al., 2007a, 2007b; Lau et al., 2008a, 2008b; Vicente, 2002). Graphical features are easier for operators to process than individual parameters, and they reveal relationships between pieces of information that are important to situation assessment. Thus, graphical displays are likely to play an important role in future control rooms. Rather than avoiding their use, the industry should seek ways to minimize the potential negative effects of sensor degradation.

Low Pressurizer Level Event	Event Occurs	Event Does Not Occur
Level Sensor Accurate	Correct Assessment	Correct Assessment
Level Sensor Fails In Normal Range	Incorrect Assessment	Correct Assessment
Level Sensor Fails Low	Correct Assessment	Incorrect Assessment
Level Sensor Fails High	Incorrect Assessment	Incorrect Assessment

Figure 4-4 Potential Relationship Between Sensor Failure and the Operator's Situation Assessment of a Low-Pressurizer-Level Event

Except for the Halden Reactor Project study (Nystad et al., 2019), most of the studies reviewed in this section had several limitations that make it difficult to generalize their findings to the operational context of interest in this document, which can be described as follows:

- *Application domain*—commercial NPPs
- *Personnel*—highly trained professional operators
- *I&C system*—commercial DI&C systems
- *HSIs*—alarm, displays, and controls presented in control rooms and local control panels

Research results are generalized most easily to this operational context when the studies consider the same types of application domains, personnel, I&C systems, and HSIs. The findings of studies conducted under different circumstances cannot be extrapolated as reliably to the target context. The studies reviewed above, for example, had the following limitations:

- *Application domain*—While the domains varied, the simulated systems were usually very simple and did not involve the complexity of real-world operations.
- *Personnel*—While some professional operators participated in the studies, most participants were students with very limited training. Unlike professional operators, they had little expertise with the systems and minimal experience with operations, and their monitoring and control strategies were evolving.
- *I&C system*—The I&C systems modeled in these studies were greatly simplified from those of a commercial NPP (e.g., they were based on a few sensors rather than hundreds of them). In addition, the application of sensor noise was often unrealistic (e.g., noise was applied equally to all sensors).
- *HSIs*—The user interfaces were very simple, lacking the complexity and number of displays found in a typical plant.

The impact of more realistic sensor degradations on the performance of highly skilled professionals, operating real-world nuclear power systems and using a full suite of control room HSIs, may well be different from what was observed in these studies. Additional research is needed to address these differences.

A variety of strategies can be used to minimize the potential impact of degradations of the sensor and monitoring subsystems on operator performance:

- Analyze the impact of I&C failures on HSIs for specific designs.
- Support monitoring of I&C systems and detection of degraded conditions, although detection is not necessarily enough to manage such conditions (Brou et al., 2007).
- Ensure information quality at the HSI.
- Distinguish directly sensed information from derived information.

These strategies are described in more detail below.

Analyze the Impact of Instrumentation and Control Failures on Human-System Interfaces for Specific Designs

I&C degradations, particularly degradations of the sensor and monitoring subsystem, can render displays difficult to interpret. Perhaps worse, they can render displays misleading, giving the impression that a process disturbance has occurred. Analyses conducted during the design process should help designers understand and minimize these potential effects. These analyses should focus on identifying the HFE-significant I&C degradations (i.e., the failure modes of the I&C system that might impact HSIs used by personnel when performing risk-important tasks).

This concern has been addressed using many methods, such as HRA (NRC, 2000) and confusion matrix analysis (Kim and Seong, 2008). These two example methods are briefly discussed below.

Recent approaches to HRA recognize that sensor failure can significantly affect an operator's situation assessment, which can in turn lead to errors of commission (e.g., Kim et al., 2005, 2008; NRC, 2000). One example of such an approach is A Technique for Human Event Analysis (ATHEANA) (NRC, 2000). The ATHEANA approach includes the identification of factors that may contribute to incorrect situation assessments, including sensor failures. The development of this approach led to efforts to predict how errors of commission could result from poor situation assessment. ATHEANA's methods are useful in the current context in that they offer possible ways to analyze sensor degradations to identify those that might lead to incorrect situation assessments.

Kim and Seong (2008) proposed another method to evaluate the potential for sensor faults to lead to incorrect situation assessments. Their method resembles classic confusion matrix analysis. It involves using a plant simulator to generate two sets of HSI information patterns: one consisting of patterns for the transients and accidents of greatest concern, and the other consisting of the patterns that would result from various types of sensor failures. The analyst compares the two sets of patterns to identify those that are very similar and could therefore lead operators to misdiagnose a sensor failure as a transient or an accident.

Since modern NPPs have many HSIs, it would take considerable effort to conduct HRA or confusion matrix analyses for all of them. Accordingly, the analyses might be applied in graded fashion, to only the human actions and HSIs that are most vital to plant safety.

Support Monitoring of Instrumentation and Control Systems and Detection of Degraded Conditions

O'Hara and Higgins (2010) developed guidelines to support operators in detecting, identifying, and managing the degradations of automatic systems (discussed in the next section of this report). Many of these guidelines address general HSI features that support operators in monitoring automation, and they apply to degraded I&C conditions. For example, they state that HSI displays should support the monitoring of the I&C system's performance, the identification of degradations in it, and troubleshooting of performance problems.

Alarms indicating degraded I&C conditions can support operators' recognition of system degradations. If the HSI includes measures of the performance of I&C subsystems, operators can monitor that performance when needed and can detect changes by comparing current performance with typical performance. As one example, the HSI might give operators details of time delays, particularly when they are longer than typical ones. NUREG-0700, Revision 2, already addresses this with respect to displaying failures (Guidelines 1.1-22, "Indication of Proper Display Operation," and 1.1-23, "Indication of Display Failure"), but the principle can be extended to the entire I&C system.

Ensure Information Quality at the Human-System Interface

One way to minimize the impact of sensor and monitoring subsystem degradations is to ensure that the correct information is displayed at the operator's HSI and to flag any suspect information. Techniques such as signal validation and analytical redundancy (calculating expected parameter values using a model of the system's performance) can be used to assess the correctness of information before displaying it. These techniques may validate information, invalidate it, or fail to determine its validity. NUREG-0700, Revision 2, contains guidance on these aspects of display design, including information on invalid data (Guideline 1.4-9), unvalidated data (Guideline 1.4-10), and analytical redundancy (Guideline 1.1-21).

Distinguish Directly Sensed Information from Derived Information

Reising and Sanderson (2002a) showed how displays can be misleading when they include both directly sensed and derived information (Figure 4-6). One way to minimize this issue may be to present these two types of information differently in displays, so that operators can readily distinguish between them. However, as DI&C systems become more and more integrated even at the sensor stage, and abundant digital sensors yield much larger volumes of data than are supplied by analog I&C systems, it will become increasingly challenging for operators to process directly sensed information. In addition, much of the safety-critical information presented to operators in digital HSIs is derived information.

4.2.2 Degraded Automation/Control and Communication Subsystems

A previous study evaluated research on the relationship between automation design and human performance, including the effects of automation degradation (O'Hara and Higgins, 2010). This section summarizes the study's general findings on automation degradation.

Automation degradations are often very difficult to detect. When an automation/control system completely fails, operators might have difficulty assessing the plant's current situation and assuming manual control of the functions previously performed by automation. An understanding of the specific reasons for such difficulty may suggest ways to minimize it. In particular, two factors make it hard for operators to detect and manage automation degradations: overreliance on automation and poor HSI design.

The first, overreliance, stems from the fact that automated systems often perform tasks independently from plant personnel. While personnel do monitor the performance of the automation, their monitoring may be compromised if the other tasks for which they are responsible impose too great a workload. This problem is exacerbated when automation is reliable, and personnel trust and depend on it to function properly. Such trust can lead to overreliance on automation (Parasuraman and Riley, 1997); that is, personnel may continue to use automation even when it does not correctly fulfill its functions and may, therefore, fail to detect its degradation.

When automation deteriorates to the point that it fails to perform properly, personnel may have to carry out tasks manually. Overreliance on automation can make it challenging for them to do so, by causing "out-of-the-loop unfamiliarity" (Lee, 2006; Wickens and Hollands, 2000)—that is, a loss of situation awareness about the behavior of the automation and the status of the systems being controlled. Thus, in addition to assuming the responsibility for automation's tasks, personnel must engage in significant situation assessments. Such unplanned transitions from automatic to manual control create high workload (Huey and Wickens, 1993) and often require a change in the concept of operations, with the roles and responsibilities of individual crew members changing to compensate for the loss of automation. Recovery from automation failure is more difficult in systems employing high levels of automation than in systems employing low levels of automation (Shen and Neyens, 2014).

The NRC study on integrating advanced HSIs into an existing NPP control room offers an example of the way in which the concept of operation may shift upon loss of automation (Roth and O'Hara, 1999, 2002). In this study, the automation considered was a computer-based procedure (CBP) for emergency operating procedures (EOPs). The CBP automated many EOP tasks formerly performed by operators, including the following:

- retrieving data and assessing its quality
- analyzing the logic for each procedural step
- keeping track of location in the procedure
- tracking continuous applicability
- assessing cautions, safety-function status trees, and fold-out page criteria

Because of the automation the CBP provided, EOPs were now executed mainly by one or two persons instead of a three-person crew, while the shift supervisor of the crew focused on planning and diagnostic activities.

The study observed crews during their training with the new systems on a full-scope simulator. The training included simulations of plant disturbances, one of which was a loss of the CBP system (i.e., a loss of automation). After the simulated scenarios were implemented, researchers interviewed the crews to learn about the impact of the new systems on their tasks, teamwork, and performance.

The researchers found that upon CBP failure, the crews transitioned to using paper EOPs and the conventional control room displays rather than the CBP displays, and EOP use shifted from a one-person activity to a three-person activity. In this study, the loss of automation occurred early in the scenario, and the crews successfully managed the transition. Also, the transition away from automation was made easier by the fact that the crews were relatively inexperienced in CBP usage, and the change brought them back to a familiar mode of operation. The transition might have been significantly more difficult if the crew's normal mode of operation was to use the CBP so that the loss of automation required them to transition to an unfamiliar mode requiring much more crew coordination and communication.

The second factor identified above as contributing to the difficulty personnel have in detecting automation degradations is the design of the HSIs used to monitor automated systems. Willems and Heiney (2002) stated, "As errors involving automation tend to be more cataclysmic and costly, the human interface has become more important than ever" (p. 3). HSIs typically provide insufficient information about the goals, current activities, and performance of an automated system (Liu et al., 2002; Lee and See, 2004; Parasuraman and Riley, 1997; Roth et al., 2004; Rook and McDonnell, 1993). Improvements in HSI design may mitigate the problem.

Control performance in an NPP depends not only on the automation/control subsystem, but also on the communication subsystem. One form of degradation that may occur in a digital communication system is an increase in time delays or lags.

Most systems have inherent time delays that stem from factors such as the following:

- the time from when a control action is taken at the HSI to when the signal reaches the actuation system
- the time it takes for the system to change in response to the control action
- the time between the change in the system's response and the change in the HSI (feedback)

Research shows that time delays affect human performance (Wickens, 1984, 1986; Wickens et al., 2004). As time delays increase, there is a decrease in closed-loop control (control based on feedback) and a shift to more difficult open-loop control strategies (based on prediction), which increasingly destabilize control. In this context, "control stability" refers to a system's response to operator inputs. When stability is high, system responses and the operator's control inputs are tightly coupled. As stability declines, system responses become progressively more unpredictable.

As the time between the operator's input and system response lengthens, closed-loop control becomes more unstable. That is, there is a drop in the value of feedback as a tool to help operators regulate their control actions. Thus, for example, an operator may initiate a control action to increase pump speed to a specified value, fail to observe a change because of a time delay, and therefore take another action to increase the pump speed when it is not warranted. The two control inputs cause a much greater increase in speed than the operator intended. Consequently, the operator then takes a control action to reduce speed but again, because of a time delay, observes no change and repeats the action, generating a greater decrease in speed

than desired. The operator's control of the pump has become unstable. Thus, when time delays destabilize closed-loop control, operators often shift to a more difficult open-loop control strategy, which is more cognitively demanding and knowledge-based (Wickens, 1984).

Lorenzo (1990) gave the following example of the effect of delayed feedback on operator behavior in a chemical plant:

> A computer-based control system was so overloaded by a process upset that it ceased to update the video terminals in the CR. Unaware that the displayed information was inaccurate, operators unknowingly moved valves to their fully open or closed limits while waiting for the display to show some response. The mis-positioned valves worsened the upset, eventually causing an emergency shutdown of the unit when some relief valves lifted. [p. 15]

These findings suggest that degradations of the I&C's communication subsystem leading to time delays may degrade the operator's performance.

The following strategies, discussed further below, may help minimize the potential impact of degradations of the automation/control and communication subsystems on operator performance:

- Support the detection and management of I&C degradation in training.
- Support the management of time delays using predictive displays.

Support the Detection and Management of Instrumentation and Control Degradation in Training

Operator training plays an important role in helping operators detect automation degradations and understanding the types of degradation that can occur. In general, training in manual operations has been found to significantly improve recovery from loss of automation (Vu et al., 2012). Similar training can be extended to the rest of the I&C system (Reising and Sanderson, 2000).

Training can provide operators with specific information so that if the I&C system becomes degraded, they do the following:

- Understand how and why it might degrade or fail.
- Understand the implications of such degradations for HSIs and their own performance.
- Monitor the I&C system's performance so as to detect and recognize degradations through control room HSIs.
- Perform recovery and compensatory actions, perhaps using procedures.
- Smoothly transition to backup systems when needed.
- Understand how degradations affect the roles and responsibilities of crew members and the concept of operations.

Furthermore, simulator training that gives operators experience with examples of automation degradation helps them deal effectively with any failures (O'Hara and Higgins, 2010). It is likely that the same type of training can help operators recognize and manage degradation in other I&C subsystems.

Support the Management of Time Delays Using Predictive Displays

Research on telerobotics (e.g., controlling robotic devices from a remote location) offers a novel way to address time delays. Telerobotic control often involves time delays, especially in space operations. To compensate for them, operators can use predictive displays that provide immediate feedback about the effect of their control actions on a system's performance, as determined from a model of the system's behavior. Predictive displays can effectively address human performance issues arising from time delays (Wu et al., 2006; Xiong et al., 2006).

4.2.3 Summary

Research on the degradation of the sensor and monitoring subsystems offers the following insights:

- Sensor degradations can make displays difficult to understand, particularly when operators use graphical displays with emergent features rather than traditional displays.
- Operators can have difficulty distinguishing between process failures and sensor failures unless the HSI is designed specifically to help them do so.
- Sensor configuration affects an operator's ability to distinguish process failures from sensor failures. The latter are easier to detect when HSIs display directly sensed rather than derived values.
- The operator's task performance declines as the magnitude of sensor noise increases. In addition, with increasing noise, operators may change their control strategies; this effect becomes more pronounced when graphical displays are used. This behavior may compensate for the decrease in the usefulness of emergent features as sensor noise increases.

Research on the degradation of automation/control subsystems reveals the following:

- Automation degradations are often very difficult to detect.
- When automation completely fails, operators may have difficulty assessing the status of the tasks that automation was performing and the systems it was controlling. They may need to take manual control of those tasks and systems, which may change the roles and responsibilities of crew members.
- Factors contributing to the difficulty of detecting and responding to automation degradations include overreliance on automation and poor HSI design.

Research on time delays shows that as time lags increase, the following occur:

- Operators' control performance declines.
- Operators' closed-loop control becomes increasingly unstable.
- Operators increasingly shift to open-loop control strategies (i.e., control based on prediction rather than feedback).

These findings should be considered within the context of the studies that generated them. Many of the studies involved students using relatively simple HSIs to monitor and control highly simplified systems. To support the findings, confirmatory research is needed using professional operators and more realistic, complex environments. Research is also needed on the effects of degradation of I&C subsystems other than those described above.

Strategies to minimize the potential impact of I&C subsystem degradations on operator performance include the following:

- Analyze the impact of I&C failures on HSIs for specific designs.
- Support monitoring of I&C systems and detection of degraded conditions.
- Ensure information quality at the HSI.
- Distinguish directly sensed information from derived information.
- Support the detection and management of I&C degradation in training.
- Support the management of time delays using predictive displays.

4.3 Analysis of Industry Operating Experience

Operating experience can provide information about the effects of degraded I&C on operator performance. The authors evaluated the information on operating experience available in studies and individual licensee event reports (LERs). The results of the evaluation are organized in the following sub-sections:

- Section 4.3.1 summarizes studies that collected and analyzed the nuclear industry's experience with DI&C degradations, focusing on their prevalence and general importance, but not specifically addressing human performance.
- Section 4.3.2 discusses studies of operating experience that addressed the human performance implications of DI&C degradations.
- Section 4.3.3 analyses several specific events involving I&C degradations for which there is information about the effects on operators.
- Section 4.3.4 summarizes the lessons learned from this analysis of operating experience.

4.3.1 Analysis of the General Prevalence and Importance of Instrumentation and Control Degradations

Both the NRC and the commercial nuclear industry have been evaluating the incidence of DI&C failures for several decades. Their findings help answer general questions, such as how frequently digital systems fail and whether the consequences are significant.

Brill (2000) evaluated the number of NPP DI&C failures based on information from LERs compiled over 5 years, starting in 1994. He found 385 events involving DI&C, which constituted 8 percent of all the LERs issued over the period. Figure 4-5 displays the distribution of DI&C failures involving hardware, software, or HSIs, the latter including personnel and procedural errors involving the DI&C systems.

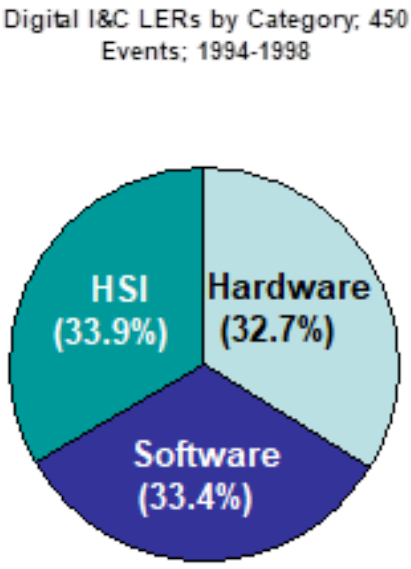


Figure 4-5 Distribution of I&C Failure Events (Source: Brill, 2000)

Many DI&C failures resulted in reactor trips (see Figure 4-6), and 36 percent of them occurred in safety-significant systems (although some of these were administrative issues, such as missed surveillance tests required by plant technical specifications).

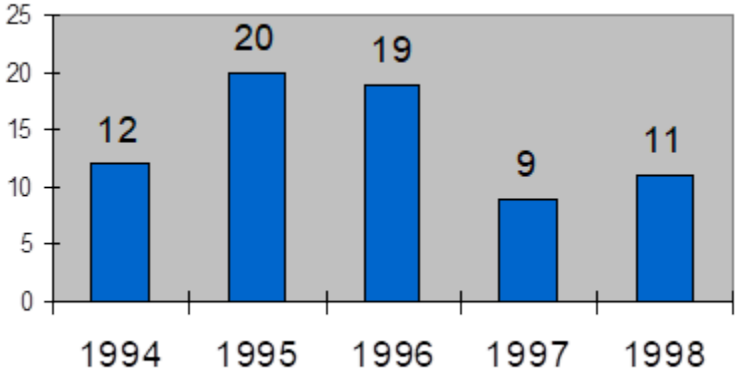


Figure 4-6 Percentage of DI&C Failures Resulting in Reactor Trips (Source: Brill, 2000)

Brill concluded that the failure of digital systems does affect plant performance and safety. This conclusion is consistent with the research of Chu et al. (2008) on the impact of failures of I&C systems on plant risk. Chu et al. (2008) studied a digital feedwater control system for a PWR, demonstrating that the potential impact of its failure on risk was primarily associated with the likelihood of a reactor trip and a significant plant transient due to a loss of feedwater.

The NRC established a database on DI&C failures (Waterman, 2006), which included data on approximately 400 DI&C failures that occurred between 1987 and 2006. Many of these events illustrate that DI&C degradation can affect human performance in the main control room, the

technical support center, and emergency operations locations. Moreover, failures have occurred in each of the I&C subsystems considered in this document. The following are examples of events that took place in 2005 or 2006 and the I&C subsystem involved:

- *Sensor subsystem*—The St. Lucie Nuclear Power Plant experienced failures on March 16 and March 19, 2006, that rendered inoperable the emergency response data acquisition and display system (ERDADS). These failures resulted in a lack of updates to the technical support center's operator consoles, leaving the displays essentially static during a training exercise.

- *Monitoring subsystem*—On June 29, 2006, St. Lucie Unit 2 exceeded the maximum power level allowed by the operating license because of a software error in the distributed control system. The software calculated a slightly lower value for feedwater flow than the actual one, and this erroneous value was used as input for the calorimetric power calculation. The error resulted in a nonconservative (lower) indicated power in the control room. Based on this faulty information, the operator increased power beyond the allowed level.

- *Monitoring subsystem*—The safety parameter display system at the Wolf Creek Generating Station was lost on June 12, 2006, because of a multiplexer failure in the link between the computer and the display panel.

- *Automation/control subsystem*—In October 2005, Byron Station, Unit 2, experienced a reactor trip. The root cause was the failure of the digital electrohydraulic system to automatically run back the turbine as designed. This was due to an application software fault that effectively rendered all automated turbine runbacks inoperable.

- *Communication subsystem*—Diablo Canyon Power Plant, Units 1 and 2, experienced a failure of the data communication system from the plant to the NRC Event Response Center in June 2006. Problems were identified in the electronics of the emergency response facility data system.

Geddes et al. (2008) analyzed data on operating experience involving DI&C degradation that was reviewed to assess the potential for common-cause failure. These data were derived from both LERs and operating experience reports from the Institute of Nuclear Power Operations. The analysis included 322 events over a period of 20 years and found the following:

- The majority (18 of 27) of common defect events in safety-related (Class IE) systems affected subsystems or channels, leaving the balance of the system unaffected and available to perform its overall safety function.
- Software changes often were implemented as corrective actions for nonsoftware problems, thereby allowing the problem to reoccur if other software changes were made.
- Most reported defects were discovered within one to two fuel cycles after the digital systems had been put into service.

Furthermore, Geddes et al. (2008) identified the following as the causes of the DI&C failures:

- inadequate design (software and hardware)
- incorrect parameter value
- hardware failure

- human performance (e.g., incorrect setpoints)
- ineffective configuration management
- inadequate testing

Geddes et al. (2008) noted that the hardware and software of DI&C systems can deteriorate, potentially affecting HSIs. In some cases, the degradations have no effect on system function, while in others they are significant. Geddes et al. (2008) also assert that "non-IE systems are more susceptible to common cause failure due to their functional complexity…[and]…their use of shared resources, e.g. power supplies." (Some of the events discussed in the next section are associated with declines in the DI&C system power supply that affected the HSI in multiple ways and thus created challenges for the operating crew.)

In summary, these studies show the following:

- DI&C degradation has occurred regularly and can be expected to increase in frequency as more digital systems are used.
- Degradations occur in all I&C subsystems.
- DI&C degradation can have major consequences (e.g., it can cause reactor trips and affect safety systems).
- Approximately a third of the DI&C degradation events recorded involved the HSI, indicating that DI&C failure could lower operators' ability to monitor the plant and respond to the event.
- Impacts were experienced in key areas, including the main control room, the technical support center, and emergency operations locations.

4.3.2 Operating Experience Studies Examining the Effects of Degraded Instrumentation and Control Conditions on Human Performance

Galletti (1996) reviewed five events involving digital systems that had implications for human performance. One event involved a degraded monitoring subsystem—specifically, a microprocessor-based overhead annunciator (OHA) system that locked up, causing the loss of alarms in the main control room. This condition went undetected by the crew for over an hour. An operator discovered it when he received an alarm on an auxiliary alarm printer and noticed that the corresponding OHA window did not alarm. Subsequent investigation revealed that the OHA system could be locked up if an operator made a particular keyboard entry when a system panel switch was mispositioned. Key contributors to the event included the following:

- *Inadequate system design*—The HSI did not adequately indicate the failure of the monitoring system.
- *Inadequate procedural guidance*—There was no procedural guidance to mitigate a loss-of-annunciator condition or to use alternative control room indications when such a condition occurred.
- *Lack of adequate operator training*—Operators were not trained to deal with a loss-of-annunciator situation. They were not aware of indications of degradation in the OHA system and were not trained to routinely verify its proper operation.

When digital systems lock up (e.g., processors either stop processing or perform infinite calculations), there may be no obvious indications for the operators. Many events can trigger

lockups, including a power interruption, voltage change, or improper operator input. Operators may be unaware that a failure has occurred because the display may have stopped at a reading within the normal operating range. Digital systems do have alarms for system failures, but the alarms may not signal all degraded conditions.

Wood et al. (2004) analyzed information from organizations involved with designing, operating, and licensing DI&C technology in new and modernized plants. One incident they analyzed involved a software error that corrupted data at the Uljin Nuclear Power Station, Unit 3, in South Korea. The failure involved an application-specific integrated circuit in a network interface module of the digital plant control system. The failure caused several non-safety components to behave unexpectedly (e.g., pumps starting and valves repositioning without a command to do so). The operators detected and responded to the situation without any negative consequences. The problem was due to a common-cause software error that was later corrected. In addition, an alarm was installed in the main control room to alert operators to possible network failures, and a procedure was written to address such situations.

The assessment of operating experience is a key aspect of the ATHEANA method for HRA (NRC, 2000). In accordance with the method, the authors of the ATHENA method analyzed selected operational events to understand human performance using theories of human cognition and human reliability models. The goals of the ATHEANA methodology are to improve the analyst's ability to do the following:

- Understand HSIs that play important roles in accident responses, including identifying and modeling errors of commission and dependencies.
- Take advantage of and integrate advances in the disciplines of psychology, engineering, plant operations, human factors, and PRA in modeling personnel actions.

ATHEANA identified certain characteristics of situations in which degraded DI&C systems could complicate operators' responses to events, including the following:

- scenarios that deviate from operators' expectations, based on their training and experience
- multiple equipment failures and unavailabilities (especially dependent or human-caused ones), beyond those represented in operator training in simulators and assumed in safety analyses
- instrumentation problems for which the operators are not fully prepared that might lead to misunderstandings about the event

The operating events reviewed in ATHEANA involved challenges to operators that were not considered in earlier risk analyses, including deviations associated with failures in instrumentation systems. Such deviations could make it difficult for operators to understand and plan suitable responses. In many cases, such deviations can lead operators to fail because of a mismatch between their expectations and plant behavior. For example, when a plant behaves in a way that is significantly different from the operators' expectations (i.e., there is a mismatch between plant behavior and training), and the operators respond in accordance with their expectations, their actions may lead to loss of equipment operation and functions that are necessary in the conditions taking place.

Table 4-1 lists several examples of degradations in the I&C sensor subsystem that affected human performance. For all these examples, the ATHENA authors concluded that incorrect

indications provided to the operators caused them to be unaware of (1) the plant's actual state, (2) the severity of plant conditions, and (3) the deterioration in plant conditions.

Table 4-1 Events Affecting Human Performance from ATHEANA

Event	Sensor Subsystem and HSI	Human Performance
Crystal River 3 (reactor coolant system pressure transient during plant startup)	Indication of the pressurizer spray valve's position was inconsistent with its actual position. There was no direct indication of pressurizer spray flow.	Situation assessment—Operators developed wrong situation model.
Dresden Unit 2 (stuck-open relief valve)	Because of a position sensor failure, the position indications for the safety relief valve showed the valve closed while it had failed open.	Situation assessment—Operators were surprised by the increase in torus temperature because they developed the wrong situation model.
Ft. Calhoun (inverter failure followed by stuck-open relief valve)	Because of the failure of a position sensor, the position indications for the safety relief valve were faulty. Also, a power supply failure degraded the computer displays normally used to monitor containment temperature and reactor coolant system cooling.	Monitoring and situation assessment—Operators had difficulty obtaining the needed information and developed the wrong situation model. Response planning was also affected because procedures did not address the incorrect position indication in adequate detail.

4.3.3 Selected Case Studies of Events Involving Digital Instrumentation and Control Degradations

The authors evaluated eight events involving DI&C degradations, focusing on their implications for human performance. Table 4-3 at the end of this section summarizes the authors' evaluation of these events. The following events received more detailed analysis since each was deemed significant in the NRC information notices issued:

- inadvertent safety injection signal with failure to reset
- degraded Ethernet communications
- failure of digital feedwater system power supplies

The first two of these events warranted special NRC inspection teams, whose reports contained more detailed information than is typically available in event reports. All three events are described below.

Inadvertent Safety Injection Signal with Failure to Reset

The failure of a single component (a Zener diode) within a protective system's logic card caused an unusual transient, so that several local manual actions were needed to reset the invalid signal and secure the safety-related equipment. The Zener diode that failed was in circuitry associated with the automatic initiation of a safety system. In the main control room, operating personnel were aware that the safety system had been initiated and determined that the initiation was spurious (not valid). However, when they reset the initiation signal, the relays did not reset everything the operators expected because the voltage had been degraded by the failed diode. In fact, the initiation signal for one safety injection train could not be reset (it was "sealed in").

This event was documented in LER 339-2007-003 (Stoddard, 2007) and NRC Information Notice (IN) 2009-03, "Solid State Protection System Card Failure Results in Spurious Safety Injection Actuator and Reactor Trip," dated March 11, 2009 (NRC, 2009b). These documents identify several instances in which the degradation of the I&C system affected the crew's performance:

- The operating crew attempted to reset both trains of the safety injection (SI), but could only reset Train A. They did not know why Train B could not be reset.
- There was no procedural guidance on how to respond to an SI signal that could not be reset from the control room.
- Motor-operated valves could not be operated from the control room, so operators had to be dispatched to manually operate them.
- A troubleshooting sheet that I&C personnel used to assist the operating crew was not sufficiently comprehensive and resulted in an incorrect configuration of the safety system's logic. This error was detected during the recovery.

The diode failure degraded the automation/control subsystem and prevented the operators from responding by taking corrective actions via their controls. Consequently, they lost situation awareness and could not rectify the abnormal situation.

The NRC special inspection report (NRC, 2007a) noted several examples of operator actions that were based on the operators' knowledge and skill of the craft, rather than procedurally driven. The inspection team also noted that "the licensee did not have a surveillance or maintenance program that was able to identify degradation of reactor protection system logic cards," nor did the licensee "have a method of trending and documenting component performance and thus identifying degraded components prior to failure."

Table 4-2 lists the sequence of events, the procedures used, the manual actions that were necessary, and the misleading information provided to the operating crew as a result of the degraded DI&C conditions.

Table 4-2 Sequence of Events for the Inadvertent Safety Injection Signal with Failure to Reset

Date: Time	Event/Action	Comment
6/29: 1752	Unit 2 main feedwater pumps tripped because of a spurious B train SI signal.	
1753	Operators manually actuated both SI trains.	Per the EOP.
1800	Operators tried to reset the SI signal from the main control room, but the B train would not reset.	Degraded voltage condition caused B train master relays to remain energized.
1810–1830	One power-operated relief valve (PORV) began lifting; pressurizer relief tank rupture disk ruptured; containment sump high-level alarm sounded; boron injection tank (BIT) valve was manually closed.	BIT valve was not operable from control because of sealed-in B train logic; PORV cycled ~50 times; 2,800 gallons of reactor coolant flowed to the containment basement.
1840	Operators restored letdown flow using guidance in abnormal procedure "Loss of Vital Instrumentation."	
1851	I&C technicians used a troubleshooting procedure to help operations reset B train SI signal.	This involved placing the mode selector switch in TEST.
1854–2058	Operating crew realigned equipment from the main control room. They could not secure the emergency diesel generator (EDG), which ran unloaded for 2 hours.	The SI signal was still present. Operations placed the EDG switch in the Emergency Stop position.
6/30: 0839	Unit 2 entered cold-shutdown mode.	Many manual valve operations were required to achieve cold shutdown.
1100	Operations personnel removed the fuses from both trains of the solid-state protection system.	This deenergized all master and slave relays so that equipment could be returned to its normal configuration.

Degraded Ethernet Communications

NRC IN 2007-15, "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," dated April 17, 2007 (NRC, 2007b), describes an event involving an overloaded Ethernet communication system linked to a recirculation pump's control system. The communication system broke down because of excessive data traffic. When the degradation occurred, the recirculating pump's speed-control demand signal fell to zero and decreased the pump's flow, resulting in a plant scram due to a potential high-power, low-flow condition. The two variable-frequency drives regulating the speed of recirculating pumps failed, necessitating a manual scram. The variable-frequency drive controllers, connected to the plant's integrated computer system network, failed because of excessive traffic on the network. The NRC issued IN 2007-15 because of the unanticipated effects of the failure of the Ethernet communication systems, which connected non-safety equipment, on the plant's safety and performance.

The degraded communication subsystem affected both the controls (recirculation pump speed controls) and HSIs; thus, the HSIs gave the operators no indication that the Ethernet was experiencing heavy data traffic and might be degraded (i.e., the HSIs lowered the operators'

situation awareness). The crew also lost the ability to implement the appropriate response because it could not control the recirculating pump's speed and flow.

The Ethernet communication system interacts with many aspects of the DI&C system and with operating personnel. The overload affected the recirculating system's controls (non-safety), which in turn caused a drop in the speed of the motor-generator set and recirculating flow, instigating a plant trip. The NRC concluded (NRC, 2007b) that "careful design and control of the network architecture can mitigate the risks to plant networks from malfunctioning devices, and improper network performance, and ultimately result in safer plant operations."

The licensee's corrective action included installing a network firewall device that limits the connections and traffic to any susceptible devices on the plant's network. IN 2007-15 states the following:

> Excessive data packet traffic on the network may cause connected devices to have a delayed response to new commands or even to lockup, thereby, disrupting normal network operations. This excessive network traffic is sometimes called a broadcast (or data) storm. A network found to be operating outside of normal performance parameters with a device malfunctioning can affect devices on that network, the network as a whole, or interfacing components and systems. The effects could range from a slightly degraded performance to complete failure of the component or system.

In this event, the communication subsystem (data highway) significantly limited the ability of the operators to control essential plant equipment.

Failure of Digital Feedwater System Power Supplies

A power supply in a digital feedwater control system (DFWCS) degraded to the point that it could not carry the required load when a secondary power supply failed. A status light on the power supply indicated that it was operating normally, so the operators were unaware of its degraded condition. Failure of the power supplies tripped both turbines of the reactor feedwater pump. In addition, the motor-driven main feedwater pump did not start automatically as it should have. The reactor tripped on low water level, and the high-pressure core spray and the reactor core isolation cooling (RCIC) pumps started automatically. However, the RCIC tripped on low suction pressure because it was misaligned, leaving the high-pressure core spray as the sole source of high-pressure injection into the vessel.

The degraded voltage condition generated difficult operating conditions, at one point allowing the operation of the main feedwater pump but then causing it to trip as the voltage fluctuated below allowable limits. Following the event, plant personnel found other problems, including the fact that the RCIC flow controller had been left in a degraded condition after maintenance without the knowledge of the operations staff.

The NRC conducted a special inspection of the plant and subsequently issued IN 2008-13, "Main Feedwater System Issues and Related 2007 Reactor Trip Data," dated July 30, 2008 (NRC, 2008a), to alert licensees to the circumstances of this event. An important way in which operators had been misled was that the indicator light of the power supply showed a normal condition, and the RCIC system's status light indicated that it was operable. Degradation of the power supply, therefore, impaired the operators' ability to assess the situation (degraded power supply) and to respond (the RCIC system was not in automatic mode).

Section 4.2.1 of this document discussed strategies for minimizing the potential effects of degraded sensor and monitoring subsystems on operator performance. One strategy was to improve HSIs to support operators in monitoring the I&C system and detecting degraded conditions. The operating experience reviewed above reinforces this recommendation. Alarms or indications are needed to support the operator's awareness of problematic conditions. The operator difficulties occurring in the three events described above could have been minimized or prevented if more information had been available to the operator:

- *Inadvertent safety injection signal with failure to reset*—An indication that the actuation logic had not reset would have led operators to take alternative actions much sooner than they did.
- *Degraded Ethernet communications*—An indication that the rate of communication had decreased significantly would have led operators to take manual action for the recirculating pumps.
- *Failure of digital feedwater system power supplies*—An indication that the power supply was not at full capacity would have led the operator to solicit maintenance support to prevent a failure.

Another strategy discussed above was to address these situations and the responses to them in operator training.

4.3.4 Summary

General evaluations of operating experience involving DI&C systems have shown that DI&C degradations occur regularly in all DI&C subsystems, and their frequency is expected to increase as new plants are built and more digital systems are used to modernize existing plants. DI&C degradations can have significant effects, compromising safety systems and causing reactor trips. Approximately one-third of the events recorded involving DI&C degradations affected HSIs (Brill, 2000), indicating that DI&C degradations could reduce operators' ability to monitor the plant, develop an accurate situation model, and properly respond to the event. The impacts of DI&C failures are not limited to the main control room; they may extend to technical support centers and emergency operations locations.

Degraded I&C systems affect several aspects of operator performance. For example, they may cause unexpected plant behavior, such as the inadvertent starting of equipment. In such cases, operators may misunderstand what is happening in the plant and develop an inaccurate situation model. Degraded I&C systems may also hamper operators' ability to implement responses, for example, by delaying responses and feedback when a communication system overloads and slows the system. Communication delays can significantly disrupt operator performance.

Furthermore, operators may be unable to monitor, detect, and understand the implications of degraded I&C conditions on plant performance because they have insufficient information about these conditions. Consequently, they may misinterpret the situation and lack awareness of the plant's state and the severity of the conditions. To prevent such problems, operators need improved alarms and better information on the key functional aspects of the I&C system and its role in the plant's response. In addition, operators need adequate training and procedures for managing degraded I&C conditions so that they can plan appropriate responses to them.

NUREG-0711 identifies the review of operating experience as an important means of ensuring that "the applicant has identified and analyzed HFE-related problems and issues in previous

designs that are similar to the current design under review." Summaries of existing problems derived from surveys of operating experience, such as NUREG/CR-6400, "Human Factors Engineering Insights for Advanced Reactors Based upon Operating Experience," issued January 1997 (Higgins and Nasta, 1997), may provide the NRC staff and applicants with more complete information about the effects of degraded conditions on operator performance.

Table 4-3 Summary of Events Involving Degraded I&C Conditions

Event Involving DI&C Degradation or Failure	I&C Subsystem	HSI Subsystem	Human Performance Impact	Comments
North Anna Unit 2, June 2007—Inadvertent SI signal with failure to reset. (LER 339-2007-003: Stoddard, 2007; NRC IN 2009-03)	Auto/Control	Control	Situation Assessment, Response Implementation	Power fluctuations to DI&C components can result in unusual failure modes.
Browns Ferry 3—Ethernet failure. (LER 296-2006-002: O'Grady, 2006; NRC IN 2007-15)	Auto/Control Communication	Control Information	Situation Assessment, Response Implementation	Electronic infrastructure (data highway) degradation.
Turkey Point Unit 3 and 4, November 1994 —EDG load sequencer failure; logic error would have prevented an auto initiation of an SI system. (LER 250-1994-005-02: Mowrey, 1995)	Auto/Control	Control	Response Planning and Implementation	Testing of logic circuitry made the equipment inoperable.
Palo Verde Unit 2, August 2005—Software problem with the core protection calculators would result in the use of the last known value in the event of a failure rather than initiating a trip signal. (LER 529-2005-004-01: Eubanks, 2006)	Monitoring	Alarm Control	Monitoring and Detection	Latent or undetected failure.
Perry, November 2007—Failures of the DFWCS power supplies caused a reactor scram with complications, including the loss of injection sources. (LER 440-2007-004-01: Allen, 2008)	Auto/Control Monitoring	Operator Support System	Situation Assessment, Response Implementation	Personnel were unaware of the degraded condition of the DFWCS power supplies.
Indian Point Station, September 2006—Degradation of the emergency notification system caused by software and hardware problems, causing an inability to activate the emergency notification sirens. (Waterman, 2006)	Auto/Control Communication	Information	Response Planning	DI&C degradation impacts extend beyond the main control room.
St. Lucie Unit 2, March 2006—Failures on the ERDADS on two occasions. (Waterman, 2006)	Auto/Control Communication	Operator support system Information	Response Planning	The loss of signal resulted in static displays.
Byron Unit 2, October 2005—Failure of the turbine digital electrohydraulic control system due to a software error. The automatic runback feature failed. (LER 455-2005-001: Kuczynski, 2005)	Auto/Control	Control	Situation Assessment, Response Implementation	Operations personnel were not aware that this feature was inoperable and did not have the ability to take the action manually.

5 ANALYSIS OF THE EFFECTS OF DIGITAL FEEDWATER SYSTEM DEGRADATION ON HUMAN-SYSTEM INTERFACES AND OPERATOR PERFORMANCE

This section presents an analysis of the failure modes of a portion of the DFWCS of an operating PWR. Previous NRC research examined the risk significance of DI&C failures with respect to this system (Chu et al., 2008). That study evaluated the use of traditional PRA methods to analyze the risk contribution of the DFWCS. Its authors developed a detailed FMEA based on information obtained from the plant. The authors of the present study extended the existing FMEA to determine how the degradation of the DFWCS could affect HSIs and operator performance.

Section 5.1 describes the key components of the DFWCS and their relationship to the DI&C system. Section 5.2 assesses how DI&C degradation could affect operator performance. Section 5.3 presents the conclusions.

5.1 Description of the Digital Feedwater Control System

This section provides a functional and physical overview of the DFWCS. The plant has two reactor coolant loops, each having a reactor coolant pump and a steam generator (S/G). The feedwater system consists of the following:

- steam-turbine-driven centrifugal S/G feedwater pumps (FWPs)
- minimum-flow control valves
- a pump-seal water system
- main feedwater-regulating valves (MFRVs)
- bypass feedwater-regulating valves (BFRVs)
- high-pressure feedwater heaters
- associated piping and instrumentation

There is one DFWCS per secondary loop. Figure 5-1 is a diagram of one reactor coolant loop, showing the associated DFWCS and the locations of the sensors. The DFWCSs of the two feedwater system trains share the sensors from the reactor coolant loops and support both automatic and manual control.

The DFWCS of each reactor coolant loop consists of two identical central processing units (CPUs): main and backup. The units run identical software to generate the control signals for the auto/manual (A/M) controllers (i.e., the FWP, main feedwater valve (MFV), and bypass feedwater valve (BFV) controllers). The main CPU provides control demands. A failover to the backup CPU may occur under certain circumstances (e.g., a large deviation between two feedwater level signals from the same S/G). Because of the importance of the feedwater control system, its design incorporates backup and manual override capabilities.

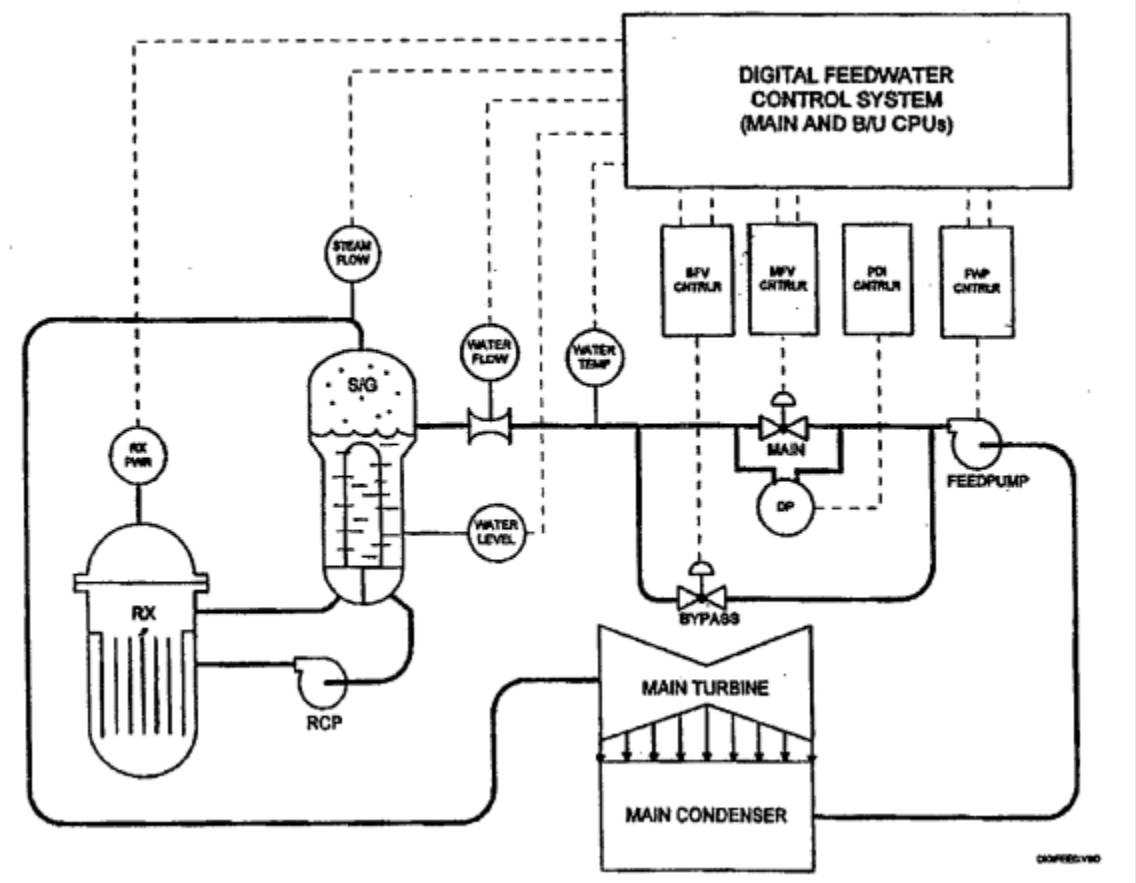


Figure 5-1 One Reactor Coolant Loop with its Associated DFWCS

Figure 5-2 shows the main components of the DFWCS (the two CPUs and the controllers); the components that are controlled (FWP, MFRV, and BFRV); the HSIs, such as the displays of the MFV, BFV, FWP, and pressure differential indication (PDI) controllers); plasma display units (PDUs); and two of the sensors supplying data to the CPUs.

An arrow indicates the passage of a signal from one component to another (e.g., from a sensor to a CPU, or from a CPU to the MFV). Some of the main signals between all these components are shown, but many others are omitted for clarity. Dotted lines represent the signals from the backup CPU, because the controllers do not use them unless the backup CPU takes control.

The DFWCS includes logic that monitors redundant input parameters for possible CPU input/output module failures or field transmitter failures. When these failures occur, the system notifies the operators and minimizes process perturbations. The logic consists primarily of deviation checks, out-of-range checks on redundant input parameters, and rate-of-change checks. The subsequent actions depend on the potential severity of the input failure modes and are tailored to the actual configuration of the plant's field transmitter.

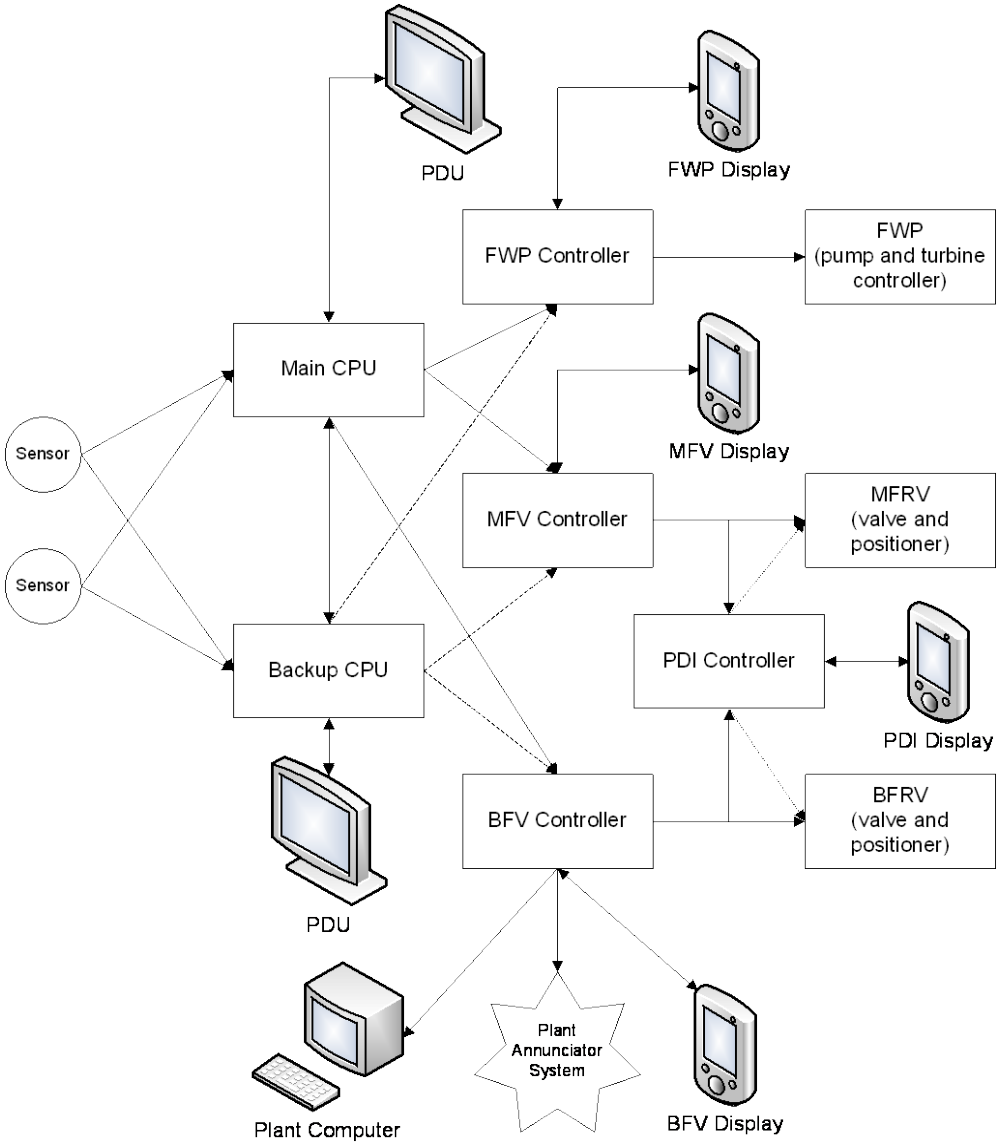


Figure 5-2 Diagram of the DFWCS and the Associated HSIs

Table 5-1 presents the relationship between the main components of the DFWCS and the I&C subsystems of the process.

Table 5-1 I&C Subsystems of the DFWCS

DFWCS Components	I&C Subsystem
Sensors	Sensor
PDUs (one for each CPU, main and backup)	Monitoring, Automation and Control
MFV, BFV, FWP, and PDI controllers	Automation and Control, Communications

Figure 5-2 illustrates the system's HSI devices. Each CPU (main and backup) has a PDU in the main control room. Each PDU acts as an input/output terminal for its CPU and is updated dynamically. The PDUs have an automatic screensaver mode that blanks the screen when no data have been entered for approximately 10 minutes (that is, no one has changed displays or entered information). Touching the screen restores the display. To prevent inadvertent data entry, the display must be completely visible before anything can be input. Alarm status indications are displayed when an operator selects them, or when a deviation alarm occurs while the display is in screensaver mode.

Each controller has a small panel display in the main control room. The display of the S/G feedwater regulating valve controller (MFV) indicates the system's status, including output demands, as well as A/M switches and increase/decrease pushbuttons for taking manual control. Secondary functions include monitoring and logic functions for actuating the main and backup CPUs, event timers, and signal deviation logic. The display offers two modes of operating an MFV controller:

- *Manual mode ("M" button pushed)*—This allows operation of the feedwater regulating valve. Usually, this mode is used when there is a problem with the DFWCS.
- *Automatic mode ("A" button pushed)*—This places the controller in automatic mode so that it automatically processes the MFV's position-demand signal. It sends the signal to the feedwater regulating valve to maintain the level of the S/G's setpoint. The controllers are normally operated automatically.

One section of the display indicates the setpoint, while another shows the actual S/G level.

The BFV controller resembles the MFV controller. However, the former also sends data to the plant annunciator system and the plant computer (PC). For example, if the system detects the failure of the main and backup CPUs, the plant annunciator alarms this condition. It also alerts the operators to several abnormal conditions in the system's operation. The PC informs the operators about the system's status under certain failure conditions. Table 5-2 shows the four types of devices making up the DFWCS HSI, along with their HSI process classifications.

Table 5-2 HSIs of the DFWCS

HSI Device	HSI Process Classification
PDUs (one for each CPU, main and backup)	Controls
MFV, BFV, FWP, and PDI controller displays	Controls
Plant annunciator system	Alarms
PC	Information System

5.2 Impact of DFWCS Degradation on Human Performance

The authors chose the MFV controller for detailed analysis of the impact of DFWCS degradation on human performance for the following reasons:

- It controls the MFRV, and failures in the position of this valve during power operation can lead to plant transients, including a reactor trip.
- The DFWCS HSIs inform the operators about the controller's status and the effects of any failures of the controller.

The analysis assumed (1) the plant is operating at full power, and (2) the DFWCS is automatically controlling feedwater in the high-power mode. During this mode of operation, the BFV is normally closed, and the DFWCS controls the MFRV and FWP.

The potential effects of the degraded I&C system on human performance were evaluated by postulating that a component of the MFV controller had degraded and propagated the degradation through the HSIs to determine its effects on human performance. The MFV controller is part of the automation and control subsystem. Listed below are the 22 degraded conditions of the MFV controller's input and output signals that were analyzed. These degradations were the failure modes identified in the FMEA for the DFWCS. Five of them, denoted by asterisks, caused a loss of automatic control of the MFRV controller, necessitating manual control. The degraded conditions analyzed are as follows:

(1) Analog Input 0 (S/G level) fails to 0.0
(2) Analog Input 1 (MFRV demand from the Main CPU) fails to 0.0*
(3) Analog Input 2 (MFRV demand from the backup [B/U] CPU) fails to 0.0
(4) Analog Output 0 (output to the MFRV positioner, PDI controller, and other S/G) fails to 0.0*
(5) Analog Output 2 (S/G level setpoint output) fails to 0.0
(6) Digital Input 0 (B/U CPU power fail or in test) fails open
(7) Digital Input 1 (B/U CPU Fail) fails open
(8) Digital Input 2 (Main CPU power fail or in test) fails open
(9) Digital Input 3 (Main CPU Fail) fails open
(10) Digital Input 0 (B/U CPU power fail or in test) fails closed
(11) Digital Input 1 (B/U CPU Fail) fails closed
(12) Digital Input 2 (Main CPU power fail or in test) fails closed
(13) Digital Input 3 (Main CPU Fail) fails closed
(14) Digital Output 0 (A/M status to the Main CPU) fails open*
(15) Digital Output 1 (A/M status to the B/U CPU) fails open
(16) Digital Output 2 (B/U CPU failed status to CPUs) fails open
(17) Digital Output 3 (Main CPU failed status to CPUs) fails open
(18) Digital Output 0 (A/M status to the Main CPU) fails closed
(19) Digital Output 1 (A/M status to the B/U CPU) fails closed
(20) Digital Output 2 (B/U CPU failed status to CPUs) fails closed
(21) Digital Output 3 (Main CPU failed status to CPUs) fails closed*
(22) Loss of power to the controller*

The results are summarized below. Table 5-4, located at the end of this section, details the potential effect of each degraded condition on the HSIs and human performance.

Seventeen of the degraded conditions are considered latent failures, because they do not cause loss of automatic control of the system but lower its functionality. If other degraded conditions occur or the operators make a mistake after a latent failure, or both, the outcome can range from negligible to severe. In 8 of these 17 degraded conditions, the HSI gives no indication that the degraded condition exists.

In 14 of the degraded conditions, one or more of the HSIs give some indication that a failure occurred. Sometimes, the HSI informs the operators only that there was a failure; it does not specify the condition. Operators generally would need technical support from maintenance personnel to troubleshoot the specific cause of the failure. One interesting case is failure mode (1) "Analog Input 0 (S/G level) fails to 0.0." The analog input 0 signal provides the S/G level to the MFV controller. The information is displayed to the operators, but the controller does not use

it for any calculations or decisions. Accordingly, this failure mode does not directly affect the system's operation. However, it will cause the displayed S/G level to be (incorrectly) low and may mislead operators to take erroneous actions to increase the S/G level (e.g., by increasing the flow of feedwater to the S/G). This can lead to a high S/G level, and should the high-level setpoint be reached, the reactor will be tripped. The likelihood of this trip is probably low because the operators would have other information that they could use to determine that this level is wrong.

As noted above, five of the degraded conditions (2, 4, 14, 21, and 22) cause a loss of automatic control of the MFRV (part of the automation and control subsystem) that requires operators to take manual control of the system. The failure to do so may result in a reactor trip due to an incorrect S/G level. In these five cases, the operators have information about the degraded condition, but the condition is not alarmed. Hence some time may elapse before they become aware of the failure, during which the problem could worsen. A reactor trip is a transient that challenges the operators and potentially the safety systems. If some components or trains are unavailable at the time of the trip, the transient may evolve into a serious safety problem (e.g., the accident at Three Mile Island Nuclear Station, Unit 2, in 1979 started with a reactor trip with a loss of feedwater). Table 5-3 lists the five conditions involving loss of automatic control of the MFRV, the impacted HSIs, and their human performance implications.

Table 5-3 Degraded MFV Conditions Resulting in Loss of Automatic Control of the MFRV

Degraded Condition		HSI	Human Performance
(2)	Analog Input 1 (MFRV demand from the Main CPU) fails to 0.0	Controls and Information Systems	The operators must take manual control of the MFRV using the PDI controller. Information about the condition is available (in the MFV controller and PC) but is not annunciated.
(4)	Analog Output 0 (output to the MFRV positioner, PDI controlled, and other S/G) fails to 0.0	Controls	The operators must take manual control of the MFRV using the PDI controller. Information about the condition is available (in the PDI controller) but is not annunciated.
(14)	Digital Output 0 (A/M status to the Main CPU) fails open	Controls and Information Systems	The operators must take manual control of the MFRV using the MFV controller. Information about the condition is available (in the PDU of the Main CPU and PC) but is not annunciated.
(21)	Digital Output 3 (Main CPU failed status to CPUs) fails closed	Controls and Information Systems	The operators must take manual control of the MFRV using the MFV controller. Information about the condition is available (in the PDU of the main CPU, MFV controller, and PC), but is not annunciated.
(22)	Loss of power to the controller	Controls and Information Systems	The operators must take manual control of the MFRV using the PDI controller. Information about the condition is available (loss of display of the MFV controller, and the PC), but is not annunciated.

As noted in Section 4.2.1 of this document, improving the HSIs is one way to minimize the potential impact of degraded sensor and monitoring subsystems on the operator's ability to detect and manage degradations. The evaluation in this section provided the following insights supporting this recommendation:

- Indications are needed to support operator awareness of degraded components. Of 17 degraded conditions involving latent failures evaluated here, 8 are not communicated to the control room.
- Five of the degraded conditions cause a loss of automatic control. Therefore, an alarm should alert the operator to the automatic/manual status of the system.

The evaluation also supports another recommendation from Section 4.2.1, namely, to assess the outcome of I&C failures on the HSIs. Extending the designer's FMEA to include how failure modes are processed through the HSI might reveal potential impacts on human performance that could be addressed in system design.

5.3 Summary

The analysis of selected failure modes in a DFWCS revealed the following:

- Sensor failures can mislead operators about the plant's state. The problem is more complex when the control system uses information different from that available to the operators. In this situation, operators may take inappropriate actions based on the erroneous information they receive.
- Significant degradation of the digital system may not be alarmed or communicated to operators in a timely way. This can cause a delayed response or possibly no response.
- Degraded conditions may lead to latent failures that do not affect the system's functionality and are not communicated to the operators. This might have serious consequences later if new failures occur or conditions change.
- Loss of automatic control places demands on operators and can lead to significant transients, such as a reactor trip.

The analysis illustrates how designers might assess the potential impacts of degradations on human performance by extending existing FMEA analyses to address how HSIs process each failure mode. For the specific case of the DFWCS, the analysis uncovered weaknesses in the HSIs and identified possible improvements.

Table 5-4 Summary of Results of Each Degraded Condition of the MFV Controller in the DFWCS

Degraded Condition		System Impact	HSI Impact	Human Performance Impact
(1)	Analog Input 0 (S/G level) fails to 0.0	The signal is for display only.	The MFV display of S/G level will be low. There is no specific alarm or message.	Information about this failure mode is not available directly. Failure can affect the operator's ability to manually control the MFRV because this indication of the S/G level is not available to the operator.
(2)	Analog Input 1 (MFRV demand from the Main CPU) fails to 0.0	The controller will initially forward the failed demand signal to the MFRV positioner, the PDI controller, and the CPUs of the other S/G. The PDI controller will then detect the signal failure and automatically become the manual controller for the MFRV. The MFRV must be manually controlled via the PDI controller.	The MFV controller will display a "DEV" (deviation) message when the main CPU's demand signal differs from that of the B/U CPU by more than a setpoint after a time delay. The deviation status will be sent to the BFV controller, which will activate a message in the PC. The PDI controller will display an "MFV Fail" message. There is no auditory alert to the operators.	The operators must take manual control of the MFRV using the PDI controller. However, since information about this failure mode is available, but not annunciated, their control actions may be delayed.
(3)	Analog Input 2 (MFRV demand from the B/U CPU) fails to 0.0	The MFV controller will continue to forward the signal from the main CPU to its output. There is no effect on the system's operation.	The MFV controller will display a "DEV" message when the main CPU's demand signal differs from that of the B/U CPU by more than a setpoint after a time delay. The "DEV" message will be sent to the BFV controller, which will activate a "System Trouble" message at the PC. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition		System Impact	HSI Impact	Human Performance Impact
(4)	Analog Output 0 (output to the MFRV positioner, PDI controller, and other S/G) fails to 0.0	The demand signal to the MFRV positioner will fail to 0, and the valve will begin to shut. The PDI controller will detect the failure and automatically transfer to the manual mode. The PDI controller's output then will rise to the pre-failure value of the MFV controller's output, and the MFRV will return to that position. The MFRV must be manually controlled from the PDI controller.	The PDI controller will display an "MFV Fail" message. Hence, information about this failure mode is available, but not annunciated.	The operators must take manual control of the MFRV using the PDI controller.
(5)	Analog Output 2 (S/G level setpoint output) fails to 0.0	The CPUs will detect a setpoint deviation if the related setpoint limit is exceeded and revert to a built-in setpoint. Hence, the system is unaffected by this failure mode.	A system deviation message in the PC will be activated if a setpoint deviation is detected. Hence, information about this failure mode is available but not annunciated. The setpoint display at the BFV controller will be low. The operator may use the MFV controller to manually adjust the SG level setpoint. However, the setpoint at the display of the BFV controller will remain low.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
(6)	Digital Input 0 (B/U CPU power fail or in test) fails open	The MFV controller will block the B/U CPU's demand signal from its output. System operation will not be affected. The B/U CPU's status is sent to the CPUs and could affect the deviation logic of the CPUs. The signal is normally closed, indicating that the B/U CPU is okay.	The MFV controller will indicate that the B/U CPU is failed by displaying the message "BCPU [backup central processing unit] Fail." The B/U CPU's status will be sent to the BFV controller that will transmit a message to the PC. Hence, information about this failure mode is available but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
(7)	Digital Input 1 (B/U CPU Fail) fails open	The controller will not be able to determine the correct status of the B/U CPU. System operation is unaffected unless other failures occur. The signal is normally open, indicating that the B/U CPU is okay.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition		System Impact	HSI Impact	Human Performance Impact
(8)	Digital Input 2 (Main CPU power fail or in test) fails open	Failover will occur from the main CPU to the B/U CPU. The MFV controller will send a Main CPU Fail signal to the CPUs and to the BFV controller. The Main CPU Fail signal affects the deviation logic of the B/U CPU. The signal is normally closed, indicating that the main CPU is okay.	The MFV controller will indicate that the main CPU is failed by displaying the message “MCPU [main central processing unit] Fail.” The BFV controller will send a message to the PC. Hence, information about this failure mode is available but not annunciated.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.
(9)	Digital Input 3 (Main CPU Fail) fails open	The controller will not be able to determine the status of the main CPU. System operation is unaffected unless other failures occur. The signal is normally open, indicating that the main CPU is okay.	There is no indication of this failure.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.
(10)	Digital Input 0 (B/U CPU power fail or in test) fails closed	The controller will not be able to determine the correct status of the B/U CPU. System operation is unaffected unless other failures occur. The signal is normally closed, indicating that the B/U CPU is okay.	There is no indication of this failure.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.
(11)	Digital Input 1 (B/U CPU Fail) fails closed	The MFV controller will block the B/U CPU’s demand signal from its output. System operation will not be affected. The B/U CPU’s status is sent to the CPUs and could affect their deviation logic. The signal is normally open, indicating that the B/U CPU is okay.	The MFV controller will indicate that the B/U CPU is failed by displaying the message “BCPU Fail.” The B/U CPU’s status will be sent to the BFV controller, which will transmit a message to the PC. Hence, information about this failure mode is available but not annunciated.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.
(12)	Digital Input 2 (Main CPU power fail or in test) fails closed	The MFV controller will be unable to determine the correct status of the main CPU. The operation of the system is unaffected unless other failures occur. The signal is normally closed.	There is no indication of this failure.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition		System Impact	HSI Impact	Human Performance Impact
(13)	Digital Input 3 (Main CPU Fail) fails closed	A failover will take place from the main CPU to the B/U CPU. The MFV controller will send a Main CPU Fail signal to the CPUs and to the BFV controller. The Main CPU Fail signal affects the deviation logic of the B/U CPU. The operation of the system is unaffected unless other failures occur. The signal is normally open, indicating that the main CPU is okay.	The MFV controller will indicate that the main CPU is failed by displaying the message “MCPU Fail.” The BFV controller will send a message to the PC. Hence, information about this failure mode is available but not annunciated.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.
(14)	Digital Output 0 (A/M status to the Main CPU) fails open	A manual signal will be sent to the main CPU, and the Transfer Inhibit Alarm window will be activated. Assuming the main CPU is in control, and the MFV controller is in automatic, the main CPU will switch to the tracking mode, tracking the MFV controller’s output. That output will be sent from the main CPU to the MFV controller. The automatic control of the MFRV effectively is lost, and the operators must take manual control using the MFV controller. The signal is normally closed in automatic mode.	The PDU of the main CPU will display the “Transfer Inhibit Alarm.” A message also will be sent to the PC. Hence, information about this failure mode is available, but not annunciated.	The operators must take manual control of the MFRV using the MFV controller.
(15)	Digital Output 1 (A/M status to the B/U CPU) fails open	Assuming the main CPU is in control and the controller is in automatic, system operation will not be affected. The signal is normally closed in automatic mode.	The PDU of the B/U CPU will display the “Transfer Inhibit Alarm.” A message also will be sent to the PC. Hence, information about this failure mode is available but not annunciated.	Since the system’s operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition		System Impact	HSI Impact	Human Performance Impact
(16)	Digital Output 2 (B/U CPU failed status to CPUs) fails open	The failed signal will be sent to the Main and B/U CPUs. Assuming the Main CPU is in control, and the MFV controller is in auto, system operation is unaffected. The signal is normally open, indicating that the B/U CPU is okay.	There is no indication of the failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
(17)	Digital Output 3 (Main CPU failed status to CPUs) fails open	The failed signal will be sent to the Main and B/U CPUs. Assuming the Main CPU is in control, the system's operation is not affected. This signal is normally open, indicating that the main CPU is okay.	There is no indication of the failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
(18)	Digital Output 0 (A/M status to the Main CPU) fails closed	The failed signal will be sent to the Main CPU. Assuming the Main CPU is in control, the system's operation is not affected. The signal is normally closed when in automatic mode.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
(19)	Digital Output 1 (A/M status to the B/U CPU) fails closed	If the Main CPU is in control, and the MFV controller is in automatic mode, then the system's operation is not affected. The signal is normally closed when the controller is in automatic mode.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition		System Impact	HSI Impact	Human Performance Impact
(20)	Digital Output 2 (B/U CPU failed status to CPUs) fails closed	The failed signal will be sent to both CPUs. The B/U CPU will continue in tracking mode. If the Main CPU is in control and the MFV controller is in automatic mode, system operation will be unaffected. The failed signal may affect the deviation logic of the Main CPU. The signal is normally open, indicating that the B/U CPU is okay.	The PDUs of the CPUs display a message indicating that the B/U CPU failed. A message also is sent to the PC. Hence, information about this failure mode is available but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
(21)	Digital Output 3 (Main CPU failed status to CPUs) fails closed	The failed signal will be sent to both CPUs. The Main CPU will enter a tracking mode and will send demand signals received from the MFV back to this controller. The MFV controller cannot detect the failure of the Main CPU when this CPU is tracking. Hence, there is a loss of automatic control of the MFRV. The signal is normally open, indicating that the main CPU is okay.	The PDU of the Main CPU will display a message indicating that the Main CPU failed. The MFV controller will show the message "MCPU Fail" and send a signal to the BFV controller, which will transmit a message to the PC. Hence, information about this failure mode is available but not annunciated.	The operators must take manual control of the MFRV using the MFV controller.
(22)	Loss of power to the controller	All analog outputs from the MFV controller fail to 0. All digital outputs from this controller fail to "Open" status. The PDI controller will switch automatically to manual mode of operation, and initially its output will rise to the pre-failure output level of the MFV controller. The MFRV must be controlled manually using the PDI controller. The CPUs will use the built-in S/G level setpoint and track PDI controller's output.	The MFV controller will be off. The PDI controller will display an "MFV Fail" message. The BFV controller possibly will send a message to the PC. Hence, information about this failure mode is available but not annunciated.	The operators must take manual control of the MFRV using the PDI controller.

6 DISCUSSION

This report presents information on degraded I&C conditions and their impact on plant and personnel performance. Even though digital systems are typically highly reliable, their potential degradation or failure could greatly affect operator performance and consequently impact plant safety. The objectives of this study were to (1) examine the effects of degraded HSI and DI&C conditions on human performance and plant operations, and (2) develop guidance for the review of HSI support for the detection and management of degraded HSI and DI&C conditions by plant personnel.

Accordingly, the authors reviewed information contained in (1) pertinent standards and guidelines, (2) HFE textbooks and basic literature, and (3) plant operating experience. In addition, they evaluated the potential effects of selected failure modes of a plant's DFWCS on the HSIs and operator performance.

The findings indicate that I&C degradations are prevalent in plants employing digital systems and can have significant effects on plant behavior, for example, by causing a reactor trip or causing equipment to operate unexpectedly. These degradations can impact the HSIs used by operators to monitor and control the plant and thus affect operator performance.

Evidence suggests that plant designers may not adequately consider the effect of HSI and I&C degradation on plant operations. For example, evaluations using FMEA methodology typically do not look at how such degradation affects control room HSIs. In general, safety analysis of plant designs typically focuses on the effect of the failure of a whole system, rather than considering what degradations might impact system functions and the quality of information presented to operators. Moreover, degradation may occur while the system continues to operate, but with impaired functioning and possibly incorrect information (e.g., from a faulty sensor). This condition is likely to be more difficult for operators to recognize. In addition, important degradations may not be alarmed, and operators may not have enough information from HSIs, in procedures, or from training to deal with them. There is literature beyond this evaluation suggesting that more detailed evaluations of the effects of I&C failures on control room HSIs are needed (Kim and Seong, 2008).

The study identified two primary strategies for addressing the human performance issues associated with degraded HSI and I&C systems. One strategy is to analyze the potential impact of I&C failures on HSIs to identify HFE-significant degradations, for example, by extending an FMEA to address how I&C failures could impact HSIs and human performance. The second strategy is to improve the HSIs so that they better support operators in monitoring the HSI and I&C systems and in detecting and managing degraded conditions.

The evaluations form the technical basis for the NRC's development of updated HFE review guidance. This guidance addresses the treatment of degraded HSI and I&C conditions as part of the design process, as well as the identification of HSI features and functions that support operators in monitoring HSI and I&C performance and managing any degradations that occur. The guidance is intended to support the NRC staff's HFE reviews of degraded and failed HSIs related to I&C systems.

6.1 The NRC's Methodology for Developing Human Factors Engineering Guidance

One contribution of this report is that it systematically documents the NRC's methodology for developing HFE guidance. The methodology consists of four steps: user needs analysis, technical basis and guidance development, peer review, and guidance integration and document publication. Section 2 of this document describes these four steps. The following discussion highlights how the methodology was applied to the topic of degraded I&C conditions.

User Needs Analysis

An NRC study conducted in 2008 identified a need for this research. The study examined human performance research issues associated with the implementation of new technology in NPPs (O'Hara et al., 2008a, 2008b). One issue identified as having top priority was "operations under conditions of degraded instrumentation and controls." Similarly, EPRI and the NEI highlighted I&C degradation as an important technical issue facing new plant development (Torok et al., 2006). Thus, both the NRC and the industry identified HSI and I&C degradation as a topic warranting further research and guidance development.

Technical Basis and Guidance Development

The authors began developing a technical basis for guidance by evaluating existing HFE standards and guidelines, such as those developed by the NRC, IEEE, and EPRI. These documents were found to emphasize the importance of conducting analyses to examine the effects of degraded conditions, designing HSIs that help operators recognize and manage degraded conditions, and offering training to ensure that operators respond properly to degraded conditions.

The authors then consulted HFE textbooks and basic literature, organizing their findings according to the I&C subsystem considered. Research on the degradation of sensor and monitoring subsystems indicated the following:

- Sensor degradations can make displays difficult to understand, particularly when operators use graphical displays with emergent features rather than traditional displays.
- Operators can have difficulty distinguishing between process failures and sensor failures unless the HSI is designed specifically to help them do so.
- Sensor configuration affects an operator's ability to distinguish process failures from sensor failures. The latter are easier to detect when HSIs display directly sensed rather than derived values.
- The operator's task performance declines as the magnitude of sensor noise increases. In addition, with increasing noise, operators may change their control strategies; this effect becomes more pronounced when graphical displays are used. This behavior may compensate for the decrease in the usefulness of emergent features as sensor noise increases.

Research on the degradation of automation and control subsystems indicates the following:

- Automation degradations are often very difficult to detect.
- When automation completely fails, operators may have difficulty assessing the status of the tasks that automation was performing and the systems it was controlling; hence they

may have trouble assuming manual control. Furthermore, an increase in manual operations changes the roles and responsibilities of crew members.

- Factors contributing to this difficulty include overreliance on automation and HSI design.

Research on communication subsystems shows that as time delays increase, the following occur:

- Operators' control performance declines.
- Operators' closed-loop control becomes increasingly unstable.
- Operators increasingly shift to open-loop control strategies (i.e., control based on prediction rather than feedback).

The literature review identified a variety of strategies that might minimize the potential impact of I&C subsystem degradations on operator performance, including the following:

- Analyze the impact of I&C failures on HSIs for specific designs.
- Support monitoring of I&C systems and detection of degraded conditions.
- Ensure information quality at the HSI.
- Distinguish directly sensed information from derived information.
- Support the detection and management of I&C degradation in training.
- Support the management of time delays using predictive displays.

Information from HFE textbooks and basic literature shows that I&C degradations can have significant effects and can adversely affect HSIs and operator performance. However, these findings should be considered within the context of the studies that generated them. Many of the studies involved students using relatively simple HSIs to monitor and control highly simplified systems. To support the findings, confirmatory research is needed using professional operators and more realistic, complex environments.

As the final step in the literature review, the authors consulted evaluations of operating experience involving DI&C systems. These evaluations show that DI&C degradations occur regularly in all DI&C subsystems, and their frequency is likely to increase as new plants are built and more digital systems are used to modernize existing plants. Approximately one-third of the events recorded involving DI&C degradations affected HSIs (Brill, 2000), indicating the DI&C failures could reduce operators' ability to monitor the plant and respond to events. The impacts of DI&C failures are not limited to the main control room; they may extend to technical support centers and emergency operations locations.

DI&C degradations can have significant effects, compromising safety systems and causing reactor trips. They may affect several aspects of operator performance. For example, they may cause unexpected plant behavior, such as the inadvertent starting of equipment. In such cases, operators may misunderstand what is happening in the plant and develop an inaccurate situation model. Degraded I&C systems may also hamper operators' ability to implement responses—for example, by delaying responses and feedback when a communication system overloads and slows the system.

Furthermore, operators may be unable to monitor, detect, and understand the implications of degraded I&C conditions on plant performance because they have insufficient information about

these conditions. Consequently, they may misinterpret the situation and lack awareness of the plant's state and the severity of the conditions. To prevent such problems, operators need improved alarms and better information on the key functional aspects of the I&C system and its role in the plant's response. In addition, operators need adequate training and procedures for managing degraded I&C conditions so that they can plan appropriate responses to them.

To complete the technical basis, the authors analyzed an existing plant's DFWCS, extending an existing FMEA to examine the potential effects of selected DFWCS failures on HSIs and operator performance. The analysis revealed the following:

- Sensor failures can mislead operators about the plant's state. The problem is more complex when the control system uses information different from that available to the operators. In this situation, operators may take inappropriate actions based on the erroneous information they receive.
- Significant degradations of the digital system may not be alarmed or communicated to operators in a timely way. This can cause a delayed response or possibly no response.
- Degraded conditions may lead to latent failures that do not affect the system's functionality and are not communicated to the operators. This might have serious consequences later if new failures occur or conditions change.
- Loss of automatic control places demands on operators and can lead to significant transients, such as a reactor trip.

The FMEA analysis of the DFWCS uncovered several weaknesses in the HSIs and identified opportunities for improvements. A similar approach may be useful in the examination of other systems and plants.

The authors used the information obtained above as the technical basis for preliminary design review guidance. The guidance was focused on (1) the HSIs used for monitoring the HSI and I&C systems and managing any degradations, and (2) an applicant's approach to addressing degraded HSI and I&C systems during the design process.

Peer Review

As the third step in the guidance development process, subject-matter experts with knowledge of HFE, I&C, and operations reviewed the preliminary guidance and evaluated its scope, comprehensiveness, technical content, technical basis, and usability. The authors revised the guidance based on their comments and suggestions.

Guidance Integration and Document Publication

As the last step in the guidance development process, the authors integrated the revised guidance into NUREG-0700, Revision 3. Because NUREG-0700, Revision 2, already contained some guidance addressing degraded and failed conditions, the authors verified whether the new guidance would overlap or replace any of the existing guidance. They evaluated each guideline in Revision 2 to determine how it should be addressed in Revision 3. This evaluation resulted in some modifications to the guidance.

6.2 Integration of Human Factors Engineering and Digital Instrumentation and Control Design Principles in the Design and Review Process

At the time of this publication, the NRC is engaged in preapplication activities with vendors proposing new and advanced designs that will likely use fully digital control rooms. In addition, modernization activities also engender new uses of DI&C and control room automation. For example, traditional plants in the United States are being modified to use DI&C for safety systems. As DI&C brings in high integration of systems and integration between humans and systems, it is important that vendors and regulators ensure plant safety by integrating the relevant aspects of their design and review processes.

The NRC has taken steps to prepare for licensing activities associated with modernized and advanced reactors, as laid out in the roadmap for review of advanced reactor applications, DANU-ISG-2022-01, "Review of Risk-Informed, Technology-Inclusive Advanced Reactor Applications—Roadmap." These activities necessarily include consideration of DI&C and HFE. Modernization efforts may involve replacing analog instrumentation and control with DI&C, as well as automating activities that were once performed manually. Regarding modernization of operating plants, DI&C-ISG-06, Revision 2, "Digital Instrumentation and Controls: Licensing Process," issued December 2018, contains interim staff guidance (ISG) for reviewing license amendment requests (LARs) associated with safety-related DI&C equipment modifications in operating plants and in new plants once they become operational. DI&C-ISG-06 indicates that, for modifications that may involve HFE considerations, "an HFE safety evaluation should be performed in accordance with SRP [NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition] Chapter 18, 'Human Factors Engineering'; NUREG-0711, 'Human Factors Engineering Program Review Model'; and NUREG-1764, 'Guidance for the Review of Changes to Human Actions,' with close coordination with the DI&C evaluation under SRP Chapter 7 [Instrumentation and Controls]."

This report presents a framework for characterizing the interrelated aspects of I&C, HSIs, and human performance. The framework brings together considerations related to DI&C and HFE in degraded I&C conditions. The guidelines developed in this project are based on this framework. The project represents an initial effort by the NRC to integrate review activities in the areas of DI&C and HFE. The U.S. nuclear industry has also been working to integrate these areas; for example, EPRI's Digital Engineering Guide (EPRI TR-3002011816) includes DI&C requirements, HFE, and HRA within the same framework in the design process (EPRI, 2021a).

6.3 Future Research

This report presents preliminary work on preventing, detecting, and managing degraded I&C conditions in digital systems. While the guidance developed supports the review of HSI designs for addressing degraded I&C conditions, additional research issues still exist. Table 6-1 lists the issues identified for future research. Findings from future studies addressing these issues may promote better understanding of the effects of DI&C degradation on operator performance and provide a technical basis for developing improved review guidance.

Table 6-1 Research Issues Pertaining to the HFE Impacts of Degraded I&C Conditions

Issue	Description
Identification of lessons learned from operating experience of the effects of DI&C degradations on performance	There is little readily available information on operating experience concerning the HFE aspects of degradations in computer-based HSIs and DI&C systems (O'Hara et al., 2008a, 2008b; Wood et al., 2004). Additional research is needed to obtain this information and to develop lessons learned that will provide a good foundation for review guidance.
Analysis methods to identify HFE-significant I&C degradations	To analyze the effects of HSI and I&C degradations in specific plant designs, applicants need to identify those that are HFE significant (i.e., that might affect HSIs used by personnel in carrying out risk-important tasks). Additional research is needed to identify methodologies for accomplishing this (e.g., HRA, FMEA, confusion matrix analysis, and misdiagnosis tree analysis) and to compare their strengths and weaknesses.
Generalization of findings on the effects of sensor degradations on performance to the target context (NPPs)	Most findings cited in this report came from studies of college students performing simplified operational tasks, using limited HSIs and very simple I&C systems. It is necessary to verify whether these findings can be extended to more realistic contexts, including realistic patterns of sensor degradation, professional operators, complex I&C systems found in real-world NPPs, and HSIs available in real-world control rooms.
Assessment of the effects of degradations of other I&C subsystems on performance	The studies on the effects of I&C degradations cited in this report are mainly limited to the sensor subsystem and automation. Details about other I&C subsystems are needed to support the development of review guidance.
Backup systems for HSI and I&C failures	Presently, the issue of backup systems for degraded HSI and I&C systems is treated piecemeal (e.g., backups for loss of CBPs). A more systematic, comprehensive approach is needed that addresses all HFE-significant degradations.
Impact of I&C system degradation on maintenance activities	The scope of this research was limited to control room operations. However, the impact that degraded digital I&C can have on human performance related to maintenance activities is also an important consideration (O'Hara et al., 1996). Research is needed to address the relationship of maintenance, human performance, and digital I&C system degradation.

7 REFERENCES

Allen, B. (2008). LER 440-2007-004-01 for Perry Nuclear Power Plant, Automatic Reactor Protection System Actuation Due to Feedwater Control Power Supply Failure. First Energy Nuclear Operating Co. ADAMS Accession No: ML080530390

Beare, A., C. Gaddy, G. Parry, and A. Singh (1991). "An approach for assessment of the reliability of cognitive response for nuclear power plant operating crews." In G. Apostolakis (Ed.), *Probabilistic Safety Assessment and Management (PSAM)*. New York, NY: Elsevier Science.

Brill, R. (2000). "Instrumentation and Control Digital System Failures in Nuclear Power Plants" Washington, DC: U.S. Nuclear Regulatory Commission, ADAMS Accession No: ML003757315

Brou, R., S. Doane, D. Carruth, and G. Bradshaw (2007). "Pilot expertise and instrument failure: Detecting failure is only half the battle." In *Proceedings of the Human Factors and Ergonomics Society 51st Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Burns, C., G. Skraaning, Jr., G. Jamieson, N. Lau, J. Kwok, R. Welch, and G. Andresen (2008). "Evaluation of ecological interface design for nuclear process control: Situation awareness effects." *Human Factors*, 50, 663–679.

Chu, T., G. Martinez-Guridi, M. Yue, J. Lehner, and P. Samanta (2008). "Traditional Probabilistic Risk Assessment Methods for Digital Systems" (NUREG/CR-6962). Washington, DC: U.S. Nuclear Regulatory Commission, October.

Dudenhoeffer, D., B. Hallbert, D. Miller, T. Quinn, S. Arndt, L. Bond, J. O'Hara, H. Garcia, D. Holcomb, R. Wood, and J. Naser (2007). "Technology Roadmap: Instrumentation, Control, and Human Machine Interface to Support DOE Advanced Nuclear Power Plant Programs" (INL/EXT-06-11862). Washington, DC: U.S. Department of Energy.

EPRI (2021a). "Digital Engineering Guide: Decision Making Using Systems Engineering" (EPRI TR-3002011816). Palo Alto, CA: Electric Power Research Institute.

EPRI (2021b). "HAZCADS: Hazards and Consequences Analysis for Digital Systems" (EPRI TR-3002016698, Rev. 1). Palo Alto, CA: Electric Power Research Institute.

EPRI (2004). "Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification" (EPRI TR-1008122). Palo Alto, CA: Electric Power Research Institute.

EPRI (2002). "Guideline on Licensing Digital Upgrades" (EPRI TR-102348). Palo Alto, CA: Electric Power Research Institute.

Eubanks, C. (2006). LER 529-2005-004-01 for Palo Verde, Unit 2, Technical Specification Required Shutdown Due to Core Protection Calculators Inoperable. Arizona Public Service Co. ADAMS Accession No: ML061930142

Galletti, G. (1996). “Human factors issues in digital system design and implementation.” In *Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*. La Grange Park, IL: American Nuclear Society.

Geddes B., T. Nguyen, D. Blanchard, and R. Torok (2008). “U.S. Commercial Nuclear Power Plant Digital I&C System Operating Experience.” Palo Alto, CA: Electric Power Research Institute.

Higgins, J., and K. Nasta (1997). “Human Factors Engineering (HFE) Insights for Advanced Reactors Based upon Operating Experience” (NUREG/CR-6400). Washington, DC: U.S. Nuclear Regulatory Commission, January. ADAMS Accession No: ML063480112

Higgins, J., J. O’Hara, P. Lewis, J. Persensky, J. Bongarra, S. Cooper, and G. Parry (2007). “Guidance for the Review of Changes to Human Actions” (NUREG-1764, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, September. ADAMS Accession No: ML072640413

Huey, B., and C. Wickens (1993). *Workload Transition: Implications for Individual and Team Performance*. Washington, DC: National Academy Press.

Hunton, P.J., R.T. England, S. Lawrie, M. Kerrigan, J. Niedermuller, and W. Jessup (2020). “Business Case Analysis for Digital Safety-Related Instrumentation & Control System Modernizations” (INL/EXT-20-59371). Washington, DC: U.S. Department of Energy.

International Atomic Energy Agency (IAEA) (1988). “Basic Safety Principles for Nuclear Power Plants” (Safety Series No. 75-INSAG-3). Vienna, Austria: International Atomic Energy Agency.

Jamieson, G., C. Miller, W. Ho, and V. Vicente (2007a). “Ecological interface design for petrochemical process control: An empirical assessment.” *IEEE Transactions on Systems, Man, Cybernetics*, 37, 906–905-920.

Jamieson, G., C. Miller, W. Ho, and V. Vicente (2007b). “Integrating task- and work domain-based work analyses in ecological interface design: A process control case study.” *IEEE Transactions on Systems, Man, Cybernetics*, 37, 887–905.

Joe, J.C., and C.R. Kovesdi (2018). “Developing a Strategy for Full Nuclear Plant Modernization” (INL/EXT-18-51366). Washington, DC: U.S. Department of Energy.

Kaarstad, M., and E. Nystad (2019). “Impact of degraded process information on operator trust.” In *Proceedings of the 29th European Safety and Reliability Conference*. Singapore: Research Publishing.

Kim, J., W. Jung, and J. Park (2005). “A systematic approach to analyzing errors of commission from diagnosis failure in accident progression.” *Reliability Engineering and System Safety,* 89, 137–50.

Kim, J., W. Jung, and Y. Son (2008). “The MDTA-based method for assessing diagnosis failures and their impacts in nuclear power plants.” *Reliability Engineering and System Safety,* 93, 337–349.

Kim, M., and P. Seong (2008). “A method for identifying instrument faults in nuclear power plants possibly leading to wrong situation assessment.” *Reliability Engineering and System Safety,* 93, 316–324.

Kisner, R., D. Holcomb, J. Mullens, T. Wilson, R. Wood, K. Korsah, M. Muhlheim, A. Quails, M. Howlader, G. Wetherington, Jr., P. Chiaro, Jr., and A. Loebl (2009). “Design Practices for Digital Communications and Workstations in Highly Integrated Control Rooms” (NUREG/CR-6991). Washington, DC: U.S. Nuclear Regulatory Commission. ADAMS Accession No: ML092740566

Kuczynski, S. (2005). LER 455-2005-001-00 for Byron Station Unit 2, Unit 2 Automatic Reactor Trip Due to Low Steam Generator Level Resulting from a Software Fault on the Turbine Control Power Runback Feature. Exelon Generation Co, LLC, Exelon Nuclear. ADAMS Accession No: ML060930493

Lau, N., Ø. Veland, J. Kwok, G. Jamieson, C. Burns, A. Braseth, and R. Welch (2008a). “Ecological interface design in the nuclear domain: An application to the secondary subsystems of a boiling water reactor plant simulator.” *IEEE Transactions on Nuclear Science*, 55, 3579–3596.

Lau, N., G. Jamieson, G. Skraaning, Jr., and C. Burns (2008b). “Ecological interface design in the nuclear domain: An empirical evaluation of ecological displays for the secondary subsystems of a boiling water reactor plant simulator.” *IEEE Transactions on Nuclear Science*, 55, 3597–3610.

Lee, J. (2006). “Human factors and ergonomics in automation design.” In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics* (3rd Edition). New York, NY: John Wiley and Sons.

Lee, J., and K. See (2004). “Trust in automation: Designing for appropriate reliance.” *Human Factors,* 46, 50–80.

Liu, Q., K. Nakata, and K. Furuta (2002). “Display design of process systems based on functional modeling.” *Cognition, Technology and Work*, 4, 48–63.

Lorenzo, D. (1990). *A Manager’s Guide to Reducing Human Errors: Improving Human Performance in the Chemical Industry*. Washington, DC: Chemical Manufacturers Association.

Moray, N., B. Jones, J. Rasmussen, J. Lee, K. Vicente, R. Brock, and T. Djemil (1993). “A Performance Indicator of the Effectiveness of Human-Machine Interfaces for Nuclear Power Plants” (NUREG/CR-5977). Washington, DC: U.S. Nuclear Regulatory Commission, January. NRC (1993). ADAMS Accession No: ML063470482

Moray, N., J. Lee, K. Vicente, B. Jones, and J. Rasmussen (1994). “A direct perception interface for nuclear power plants.” In *Proceedings of the Human Factors and Ergonomics Society 38th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Mowrey, C. (1995). LER 250-1994-005-02 for Turkey Point Units 3 and 4, Design Defect In Safeguards Bus Sequencer Test Logic Places Both Units Outside The Design Basis. Florida Power and Light Co. ADAMS Accession No: ML17353A295

NRC (2023). “Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants” (Regulatory Guide 1.152, Rev. 4). Washington, DC: U.S. Nuclear Regulatory Commission, July. ADAMS Accession No: ML23054A463

NRC (2018). “Digital Instrumentation and Controls Licensing Process” (DI&C-ISG-06, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission, December. ADAMS Accession No: ML18269A259

NRC (2016a). “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (NUREG-0800), Chapter 18, “Human Factors Engineering” (Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission, December. ADAMS Accession No: ML16125A114

NRC (2016b). “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (NUREG-0800), Chapter 7, “Instrumentation and Controls” (Rev. 7). Washington, DC: U.S. Nuclear Regulatory Commission, August. ADAMS Accession No: ML16020A049

NRC (2015). “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (NUREG-0800), Section 19.0, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors” (Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission, December. ADAMS Accession No: ML15089A068

NRC (2014). “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (NUREG-0800), Chapter 8, “Electric Power.” Washington, DC: U.S. Nuclear Regulatory Commission. ADAMS Accession No: ML14114A430

NRC (2011). “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants” (Regulatory Guide 1.152, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission, July. ADAMS Accession No: ML102870022

NRC (2010). “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems” (Regulatory Guide 1.47, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, February. ADAMS Accession No: ML092330064

NRC (2009a). “Highly-Integrated Control Rooms—Communications Issues (HICRc)” (DI&C-ISG-04, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, March 6. ADAMS Accession No: ML083310185

NRC (2009b). “Solid State Protection System Card Failure Results in Spurious Safety Injection Actuation and Reactor Trip” (Information Notice 2009-03). Washington, DC: U.S. Nuclear Regulatory Commission, March 11. ADAMS Accession No: ML083080368

NRC (2008a). “Main Feedwater System Issues and Related 2007 Reactor Trip Data” (Information Notice 2008-13). Washington, DC: U.S. Nuclear Regulatory Commission, July 30. ADAMS Accession No: ML080880115

NRC (2008b). “Highly-Integrated Control Rooms—Human Factors Issues (HICR—HF)” (DI&C-ISG-05, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, August 11. ADAMS Accession No: ML082740440

NRC (2008c). “Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments: Interim Staff Guidance” (DI&C-ISG-03, Rev. 0). Washington, DC: U.S. Nuclear Regulatory Commission, August 11. ADAMS Accession No: ML080570048

NRC (2007a). “North Anna Power Station, Unit 2; Special Inspection Report 05000339/2007009." Washington, D.C.: U.S. Nuclear Regulatory Commission. ADAMS Accession No: ML072410359

NRC (2007b). “Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations” (Information Notice 2007-15). Washington, DC: U.S. Nuclear Regulatory Commission, April 17. ADAMS Accession No: ML071010303

NRC (2007c). “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (NUREG-0800), Chapter 8, Branch Technical Position 8.5, “Supplemental Guidance for Bypass and Inoperable Status Indication for Engineered Safety Features Systems,” Rev. 3. Washington, DC: U.S. Nuclear Regulatory Commission. ADAMS Accession No: ML070710466

NRC (2002). “Use of EPRI/NEI Joint Task Force Report, ‘Guideline on Licensing Digital Upgrades’: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule” (Regulatory Issue Summary 2002-22). Washington, DC: U.S. Nuclear Regulatory Commission, November 25. ADAMS Accession No: ML023160044

NRC (2000). “Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)” (NUREG-1624, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, May. ADAMS Accession No: ML003719212

Nystad, E., M. Kaarstad, and R. McDonald (2019). “Crew decision-making in situations with degraded information.” In *Proceedings of the 29th European Safety and Reliability Conference*. Singapore: Research Publishing.

O'Grady B (2006). LER 296-2006-002-00 for Browns Ferry, Unit 3, Manual Reactor Scram Due to Loss of the Reactor Recirculation Pumps. Tennessee Valley Authority. ADAMS Accession No: ML062900106

O’Hara, J. (2004). “Identifying and addressing lessons learned from plant modernization programs guidelines for control room modernization.” *Nuclear Plant Journal*, 22, 47–48.

O’Hara, J. (1994). “Advanced Human-System Interface Design Review Guideline” (NUREG/CR-5908). Washington, DC: U.S. Nuclear Regulatory Commission, July. ADAMS Accession No: ML071210321

O’Hara, J., and W. Brown (2002). “The Effects of Interface Management Tasks on Crew Performance and Safety in Complex, Computer-Based Systems” (NUREG/CR-6690). Washington, DC: U.S. Nuclear Regulatory Commission, August. ADAMS Accession No: ML022520381

O'Hara, J., W. Brown, P. Lewis, and J. Persensky, J. (2002). "Human-System Interface Design Review Guidelines" (NUREG-0700, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission, May.

O'Hara, J., and S. Fleger (2020). "Human-System Interface Design Review Guidelines" (NUREG-0700, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission, July. ADAMS Accession No: ML20162A214

O'Hara, J., W. Gunther, and G. Martinez-Guridi (2010). "The Effects of Degraded Digital Instrumentation and Control Systems on Human-System Interfaces and Operator Performance" (BNL-91047-2010). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., and J. Higgins (2017). "Adaptive Automation: Current Status and Challenges" (Draft BNL-D0013-1-2016). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., and J. Higgins. (2010). "Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis" (BNL-91017-2010). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., J. Higgins, W. Brown, R. Fink, J. Persensky, P. Lewis, J. Kramer, A. Szabo, and M. Boggi (2008a). "Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants" (NUREG/CR-6947). Washington, DC: U.S. Nuclear Regulatory Commission, October. ADAMS Accession No: ML083090338

O'Hara, J., J. Higgins, W. Brown, and R. Fink (2008b). "Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants: Detailed Analyses" (BNL-79947-2008). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., J. Higgins, S. Fleger, and P. Pieringer (2012). "Human Factors Engineering Program Review Model" (NUREG-0711, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission, November. ADAMS Accession No: ML12324A013

O'Hara, J., J. Higgins, and J. Kramer (2000). "Advanced Information Systems: Technical Basis and Human Factors Review Guidance" (NUREG/CR-6633). Washington, DC: U.S. Nuclear Regulatory Commission, March. ADAMS Accession No: ML003704877

O'Hara, J., and E. Roth (2005). "Operational concepts, teamwork, and technology in commercial nuclear power stations." In C. Bowers, E. Salas, and F. Jentsch (Eds.), *Creating High-Tech Teams: Practical Guidance on Work Performance and Technology*. Washington, DC: American Psychological Association.

O'Hara, J., W. Stubler, and J. Higgins (1996). "Hybrid Human-System Interfaces: Human Factors Considerations" (BNL-J6012-T1-4/96). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., W. Stubler, J. Higgins, and J. Kramer (2000). "Hybrid human-system interfaces: Trends and challenges." In *Proceedings of the Third American Nuclear Society International Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*. La Grange Park, IL: American Nuclear Society.

Parasuraman, R., and V. Riley (1997). “Humans and automation: Use, misuse, disuse, abuse.” *Human Factors*, 39, 230–253.

Reising, D., and P. Sanderson (2004). “Minimal instrumentation may compromise failure diagnosis with an ecological interface.” *Human Factors*, 46, 316–333.

Reising, D., and P. Sanderson (2002a). “Work domain analysis and sensors I: Principles and simple example.” *International Journal of Human-Computer Studies*, 56, 569–596.

Reising, D., and P. Sanderson (2002b). “Work domain analysis and sensors II: Pasteurizer II case study.” *International Journal of Human-Computer Studies*, 56, 597–637.

Reising, D., and P. Sanderson (2000). “Testing the impact of instrument location and reliability on ecological interface design: Fault diagnosis performance.” In *Proceedings of the IEA 2000/HFES 2000 Congress.* Santa Monica, CA: Human Factors and Ergonomics Society.

Rook, F., and M. McDonnell (1993). “Human cognition and the expert system interface: Mental models and inference explanations.” *IEEE Transactions on Systems, Man, and Cybernetics*, 23, 1649–1661.

Roth, E., M. Hanson, C. Hopkins, V. Mancuso, and G. Zacharias (2004). “Human in the loop evaluation of a mixed-initiative system for planning and control of multiple UAV teams.” In *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting.* Santa Monica, CA: Human Factors and Ergonomics Society.

Roth, E., R. Mumaw, and P. Lewis (1994). “An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies” (NUREG/CR-6208). Washington, DC: U.S. Nuclear Regulatory Commission, July. ADAMS Accession No: ML102571850

Roth, E., and J. O’Hara (2002). “Integrating Digital and Conventional Human-System Interfaces: Lessons Learned from a Control Room Modernization Program” (NUREG/CR-6749). Washington, DC: U.S. Nuclear Regulatory Commission, September. ADAMS Accession No: ML102571847

Roth, E., and J. O’Hara (1999). “Exploring the impact of advanced alarms, displays, and computerized procedures on teams.” In *Proceedings of the Human Factors and Ergonomics Society—43rd Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Shen, S., and D. Neyens (2014). “Assessing drivers’ performance when automated driver support systems fail with different levels of automation.” In *Proceedings of the Human Factors and Ergonomics Society—58th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

St-Cyr, O. (2006). “Impact of sensor noise magnitude on emergent features of ecological interface designs.” In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

St-Cyr, O., and K. Vicente (2005). “Sensor noise and ecological interface design: Effects of increasing noise magnitude on operators’ performance.” In *Proceedings of the Human*

Factors and Ergonomics Society 49th Annual Meeting. Santa Monica, CA: Human Factors and Ergonomics Society.

St-Cyr, O., and K. Vicente (2004). “Sensor noise and ecological interface design: Effects on operators’ control performance.” In *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Stoddard, D. (2007). LER 339-07-003-00 for North Anna, Unit 2, Automatic Reactor Trip Due to Invalid Safety Injection Relay Actuations. Virginia Electric & Power Co (VEPCO). ADAMS Accession No: ML072480671

Torok, R., J. Naser, L. Sandell, and T. Harris (2006). “I&C issues for new nuclear plant deployment.” In *Proceeding of the 16th Annual Joint POWID/EPRI Controls and Instrumentation Conference 49th Annual ISA POWID Symposium*. Research Triangle Park, NC: International Society of Automation.

Vicente, K. (2002). “Ecological interface design: Progress and challenges.” *Human Factors*, 44, 62–78.

Vicente, K., N. Moray, J. Lee, J. Rasmussen, B. Jones, R. Brock, and T. Djemil (1996). “Evaluation of a Rankine cycle display for nuclear power plant monitoring and diagnosis.” *Human Factors*, 38, 506–521.

Vicente, K., and J. Rasmussen (1992). “Ecological interface design: Theoretical foundations.” *IEEE Transactions on Systems, Man, and Cybernetics*, 2, 589–606.

Vu, K.-P. L., H. Silva, J. Ziccardi, C. Morgan, and G. Morales (2012). “How Does Reliance on Automated Tools During Learning Influence Students' Air Traffic Management Skills When the Tools Fail?” In *Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Waterman, M. (2006). Unpublished database of digital I&C failures from 1987–2006. Washington, DC: U.S. Nuclear Regulatory Commission.

Wickens, C. (1986). “The effects of control dynamics on performance.” In K. Boff, L. Kaufman, and J. Thomas (Eds.), *Handbook of Perception and Human Performance*. New York, NY: John Wiley and Sons.

Wickens, C. (1984). *Engineering Psychology and Human Performance*. Columbus, OH: Merrill Publishing Company.

Wickens, C., and J. Hollands (2000). *Engineering Psychology and Human Performance* (3rd Edition). Upper Saddle River, NJ: Prentice-Hall.

Wickens, C., J. Lee, Y. Liu, and S. Gordon (2004). *Human Factors Engineering* (2nd Edition). Upper Saddle River, NJ: Prentice Hall.

Willems, B., and M. Heiney (2002). “Decision Support Automation Research in the En Route Air Traffic Control Environment” (DOT/FAA/CT-TN02/10). Washington, DC: Federal Aviation Administration.

Wood, R., J. Easter, W. Korsah, and G. Remley (2004). “Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants” (NUREG/CR-6842). Washington, DC: U.S. Nuclear Regulatory Commission, April. ADAMS Accession No: ML041910046

Wu, Q., Z. Wang, and Z. Wang (2006). “Experiments on Stewart platform teleoperation with predictor display.” In *Sixth International Symposium on Instrumentation and Control Technology: Sensors, Automatic Measurement, Control, and Computer Simulatio*n. Bellingham, WA: SPIE.

Xiong, Y., S. Li, and M. Xie (2006). “Predictive display and interaction of telerobots based on augmented reality.” *Robotica*, 24, 447–453.

APPENDIX A DESIGN REVIEW GUIDELINES FOR HUMAN-SYSTEM INTERFACE

This appendix presents the human factors engineering (HFE) review guidance for degraded human system interface (HSI) and instrumentation and control (I&C) conditions. The guidance became Section 14, “Degraded HSI and I&C Conditions,” in NUREG-0700, Revision 3, “Human-System Interface Design Review Guidelines,” issued July 2020. The guidance includes a topic characterization for degraded HSI and I&C conditions, the review criteria for evaluating the HSIs, and a bibliography that includes the source-coded documents and other references with additional information about the topic. For ease of cross-referencing, this appendix includes the numbering from NUREG-0700, Revision 3. Note that there may be minor editorial differences between the text in this appendix and the guidance in NUREG-0700, Revision 3.

A.1 Characterization of Degraded Human-System Interface and Instrumentation and Control Conditions

Modern digital instrumentation and control (DI&C) systems provide a great deal of functionality that is vital to plant performance and safety. In all nuclear power plants, personnel interact with the instrumentation and control (I&C) system through the HSIs provided in the control room and elsewhere in the plant. Together, plant personnel and the I&C system work to perform functions that include the following:

- sensing basic parameters and statuses
- adjusting operations as needed
- responding to transients, accidents, and other failures
- monitoring plant processes and performance, as well as various barriers that prevent the release of radioactive material

DI&C systems provide added functionality compared to analog systems and can perform sophisticated monitoring, diagnostic, and prognostic functions. Diagnostics refers to techniques for identifying and determining the causes of deviations or faults in the plant’s systems or processes. Prognostics refers to methods for using sensor data to estimate the rate of physical degradation and the remaining useful life of systems, predicting time to failure, and applying this information to more effectively control processes.

DI&C systems also provide more integrated control of plant systems and processes (as opposed to separate, noninteracting control loops). They can be used to implement advanced control algorithms that enable more granular control of plant systems and processes than is possible in analog systems. Furthermore, DI&C systems support new forms of automation that make for unique interactions between plant systems and personnel.

Several subsystems, including the sensor, monitoring, automation and control, and communication subsystems, support the functionality of the I&C system.

Operators monitor and interact with the plant using the HSIs provided through the I&C system.[8] Figure A-1 illustrates the relationships among plant personnel, HSIs, and I&C subsystems.

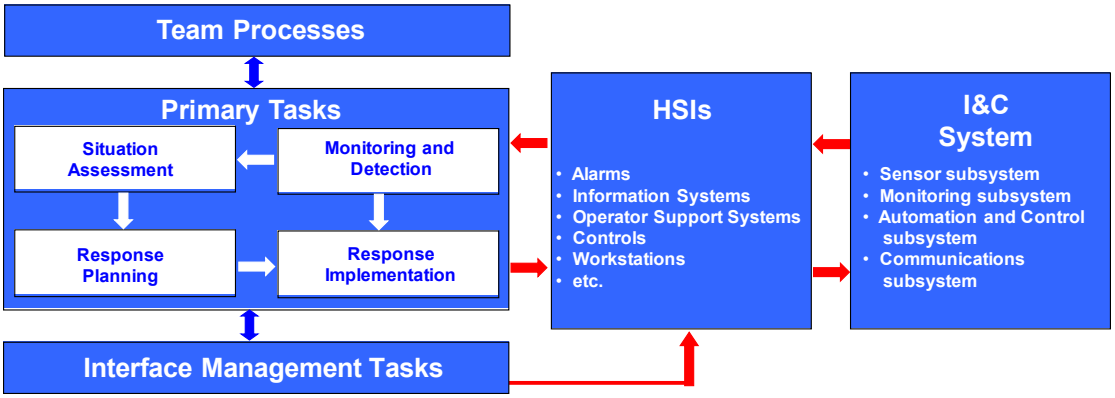


Figure A-1 Characterization of the I&C System, HSIs, and Human Performance

Each I&C subsystem and each HSI is at risk of undergoing degradation or failure. Degradation refers to a full range of conditions, from relatively minor loss of functionality to complete system failure. HSI and I&C degradation can significantly reduce the operators' ability to perform their tasks, thus threatening plant safety. It can also cause abnormal operating conditions due to erroneous automatic action or indication.

Some human-performance considerations in addressing operations under degraded I&C conditions include the following:

- monitoring the health of the HSI and I&C systems
- detecting degrading conditions and distinguishing them from process failures
- managing degraded conditions including the need to transition to backup systems when degraded conditions result in loss of needed functionality, such as in a failure

The review guidance in this section focuses on the HSI characteristics that support these activities. The guidance is organized into the following sections (the numbers match the section numbers in NUREG-0700, Revision 3):

14.1 HSIs for Monitoring I&C System Conditions
14.2 HSI Response to I&C System Changes
14.3 Information Source and Quality
14.4 Backup of HSI and I&C Failures

Additional information about degraded HSIs and I&C systems can be found in Appendix B.5 to NUREG-0700, Revision 3. Appendix B to NUREG-0700 contains guidance on selected HSI topics. U.S. Nuclear Regulatory Commission reviewers can address these considerations on a

[8] While personnel rely considerably on HSIs, they do directly monitor and take control actions in some cases, such as when observing a leak, hearing a vibration, or manipulating a manual valve.

case-by-case basis during specific reviews. The process guidance for degraded HSIs and I&C systems is organized into the following sections in Appendix B.5 to NUREG-0700, Revision 3:

B.5.1 Operating Experience Review
B.5.2 Task Analysis
B.5.3 Treatment of Important Human Actions
B.5.4 Human-System Interface Design
B.5.5 Training Program Development
B.5.6 Human Factors Verification and Validation

Bibliography

Source Code Documents

0700 U.S. Nuclear Regulatory Commission (1981). "Guidelines for Control Room Design Reviews" (NUREG-0700, Rev. 0). Washington, DC: U.S. Nuclear Regulatory Commission, September.

0835 U.S. Nuclear Regulatory Commission (1981b). "Human Factors Acceptance Criteria for the Safety Parameter Display System" (NUREG-0835). Washington, DC: U.S. Nuclear Regulatory Commission, October.

1342 Lapinsky, G., R. Eckenrode, P. Goodman, and R. Correia (1989). "A Status Report Regarding Industry Implementation of Safety Parameter Display Systems" (NUREG-1342). Washington, DC: U.S. Nuclear Regulatory Commission, April.

6633 O'Hara, J., J. Higgins, and J. Kramer (2000a). "Advanced Information Systems Design: Technical Basis and Human Factors Review Guidance" (NUREG/CR-6633). Washington, DC: U.S. Nuclear Regulatory Commission, March.

6634 O'Hara, J., J. Higgins, and J. Kramer (2000b). "Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance" (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission, March.

7264 O'Hara, J., W. Gunther, G. Martinez-Guridi, and T. Anderson, J. Xing, and S. Morrow (2025). "Managing the Effects of Degraded Instrumentation and Control Conditions on Operator Performance " (NUREG/CR-7264). Washington, DC: U.S. Nuclear Regulatory Commission.

A.2 14.1, "HSIs for Monitoring I&C System Conditions"

14.1-1 Overall Representation of the Instrumentation and Control System and Subsystems

The HSI should provide a graphical representation of the I&C system and its subsystems.

Additional Information: The representation of the I&C system and its subsystems should be sufficiently detailed to enable operators to monitor its performance and detect HSI and I&C degradations, especially those affecting important human actions, as identified in NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," issued November 2012.[7264]

14.1-2 Hierarchic Access to Information

Information should be presented in a hierarchy that enables users to quickly and easily determine the overall status of I&C systems and subsystems from top-level displays and to access more detailed information on lower-level displays.

Additional Information: Information hierarchies give operators a way to monitor the I&C system's status at a glance to verify that plant conditions are stable, to progressively access more detailed information to support their situation assessment and to perform any required troubleshooting. The displays should contain navigation aids to enable users to quickly and easily move from high-level displays to low-level displays in the hierarchy (see NUREG-0700, Section 2.5.1, "Display Selection and Navigation").[7264]

14.1-3 Indicate Important Status and Performance Parameters

The HSI should provide information about each I&C subsystem's status and performance parameters.

Additional Information: The intent of this guideline is to give operators knowledge about how well the HSI and I&C system are performing. If the HSI and I&C system include status and performance information for HSI and I&C subsystems, operators can monitor that performance. Comparing current performance with expected performance will help operators detect degradation in the system. HSI and I&C systems that have continuous online self-testing and monitoring/trending capabilities will allow operators to promptly identify degradations (see Guidelines 13.8.2.2-1 and 13.1.3-1 in NUREG-0700 for additional information).[7264]

14.1-4 Indication of Proper Human-System Interface and Instrumentation and Control System Operation

A display feature should be provided to indicate to the user that the HSIs and the I&C system are operating properly.

Additional Information: For example, a display of calendar date and time can be used to indicate whether a computer display is functioning. A built-in testing feature may be used to routinely assess operability of the system.[0700]

14.1-5 User-Requested Status Check

The HSI should allow users to request an HSI or I&C system check without adversely impacting plant operations.

Additional Information: If users suspect that the HSIs or I&C system may not be working properly, requesting a status check without adversely impacting plant operations may help resolve the concern. This is especially important for checking automation systems.[7264]

A.3 14.2, "HSI Response to I&C System Changes"

14.2-1 Notification of Important Changes

The HSIs should notify users of important changes in I&C system status, performance, and degrading conditions.

Additional Information: Alerts should be graded based on the need for the operator's action (e.g., if immediate action is needed, an alarm should be used). I&C system indications are especially important for systems that fail without producing immediately noticeable changes in the plant's behavior. In a degraded condition, the I&C system may still carry out its function, but its performance is not optimal. The communication subsystem provides an example. Operators should be alerted if time delays slow the update of information displays and responses to control inputs. The following are additional examples of degraded conditions that should be indicated:

- loss of redundancy (until the redundant system, equipment, module, or component becomes operable again)
- overload indications (even if the equipment continues to operate when overloaded)
- out-of-range indicators
- power failure indicators (i.e., a power-on indicator that extinguishes with loss of power); an indication should be provided if a fuse or breaker has opened a circuit
- automation degradation (automation should communicate degradations to personnel promptly to engage them more fully in the responsibilities of the automation)

Depending on the nature of the alerts, they should be routed to the most appropriate destinations (e.g., control room operators or maintenance personnel). (See NUREG-0700, Section 4.1.4, "Alarm Routing," for additional information.)[7264]

14.2-2 Indication of Information Inaccuracy

Information system failures (caused by sensors, instruments, and components) should result in distinct display changes, which directly indicate that depicted information is not valid.

Additional Information: The information system should be designed so that operators can readily recognize failures in instrumentation. When panel instruments such as meters fail or become inoperative, the failure should be apparent to the user (e.g., through offscale indication).[6633]

14.2-3 Alarm to Human-System Interface and Instrumentation and Control System and Subsystem Failure

The HSI should alarm when a failure of the HSI and I&C system and subsystem occurs.

Additional Information: In the context of this guideline, when the I&C system or subsystem performance has degraded to the point that it cannot meet its function, it is considered a failure. When the failure reflects an HFE-significant I&C degradation, the operator should receive an alarm. As with all alarms, operators should be given timely alerts, so they can take compensatory actions or use backup procedures.[7264]

14.2-4 Information on Degraded Condition and Failure Cause

The HSI should support users in determining the cause(s) of degraded conditions and failures.

Additional Information: For example, automation can mask failures and degraded conditions in other plant systems when it compensates for them. This can lead the operator to lose situation awareness and can become problematic at the point when automation no longer compensates, and operator action is required to protect the plant.[7264]

A.4 14.3, "Information Source and Validity"

14.3-1 Identify Information Source

The HSI should support operators in distinguishing between displayed information that is user entered, directly sensed, derived, or synthetic.

Additional Information: The effect of degraded I&C conditions can be more difficult to understand when displayed information comes from different sources. Four types of information can be displayed on plant HSIs: user entered, directly sensed, derived, and synthetic. Some information displayed in the HSI can be entered by users. Directly sensed information is obtained from a sensor measurement (e.g., the flow out of a tank based on a flow sensor in the output pipe). Derived information is displayed information that could be based directly on sensor measurement but instead is derived from the measurements of other sensors. For example, the flow into a tank might not be directly sensed but can be assessed from a change in level over time. Synthetic information represents higher order information about a plant that cannot be sensed directly but is computed mathematically from data gained from sensors (e.g., rate of change, mass balance). The overall status of a safety function may represent synthetic information based on a computation from the function's key safety parameters. Any such data used in these calculations from degraded or faulty sensors may propagate to the synthetic parameter and distort its meaning. One way to minimize this concern is to distinguish between these sources in a display, so operators can readily determine whether information is directly sensed or is derived from sensors.[7264]

14.3-2 Data Validation

Data presented in the HSI should be validated in real time, where possible.

Additional Information: The HSI should not give false indications of plant status; therefore, methods should be used to ensure that data are reliably presented to the operators. One approach to minimizing the impact of a degraded sensor and monitoring subsystem is to make sure that the information displayed at the operator's HSI is correct and to evaluate the correctness of suspect information. Techniques such as range checks for failed instruments, signal validation, and analytical redundancy can be used to evaluate the correctness of information before it is displayed. Range checks for failed instruments can ensure that failed instruments are identified and that their readings are not averaged with other valid readings, possibly masking their failure. Comparing and possibly averaging redundant instruments can improve the quality and reliability of data. Analytical redundancy refers to the comparison of measured sensor readings, using mathematical models based on known physical relationships among parameters, to determine whether there are inconsistencies in the values. For example, "reactor power," "reactor coolant temperature rise through the reactor core," and "reactor coolant flow rate" are interrelated parameters based on the physical principles of heat transfer. A measured value for coolant flow should be consistent with the analytically calculated value for coolant flow derived from the corresponding measured values of reactor power and coolant temperature rise.[0835, 1342, 7264]

14.3-3 Invalid Data

Parameters that are subject to validation (e.g., checks for accuracy) should be identified, and an indication should be provided when these data are invalid.

Additional Information: When data fail to meet the specified criteria for validity and thus are suspected of being of poor quality, validation failure should be indicated.[7264]

14.3-4 Unvalidated Data

When data accuracy cannot be checked, the unvalidated status of the data should be clearly indicated.

Additional Information: When checks for accuracy cannot be performed (e.g., a processor or redundant sensors are not available), the data are unvalidated. The data validation process can determine whether unvalidated data is valid or invalid. Under some conditions, trained users may find unvalidated data helpful in determining both the safety status of the plant and whether human intervention is needed. Clear indications of the unvalidated status of the data should be provided so that the operators can exercise judgment in interpreting them.[7264]

14.3-5 Display of Data Reliability and Validation

The status of information should be displayed to the operator with an appropriate quality indicator (e.g., valid, invalid, unvalidated, or numerical estimate).

Additional Information: Operators should also have available (e.g., on a separate display page) the individual sensor readings, so they can isolate an indicated problem if the validation fails.[0835]

A.5 14.4, "Backup of HSI and I&C Failures"

14.4-1 Backup System Availability

Backup systems should be available for HSI and I&C system failures [7264, 6634]

14.4-2 Support Failure Recovery and Transition to Backup Systems

The HSI should support operators in determining the steps for failure recovery or backup actions if recovery is not possible.

Additional Information: When a failure of automation is detected, the HSI should provide displays and information that allow personnel to rapidly determine what actions they must take to respond. For example, a procedure might be developed describing the appropriate response to various HSI and I&C failures. As another example, the HSI for an automated process that fails to manual mode should alert personnel that manual control is now required and point to or directly display the actions or procedures necessary to carry out the required manual actions.[7264, 6634]

APPENDIX B DESIGN PROCESS REVIEW GUIDELINES

This appendix contains the design process review guidance that became Section B.5 of NUREG-0700, Revision 3, "Human-System Interface Design Review Guidelines," issued July 2020 (O'Hara and Fleger, 2020). For ease of cross-referencing, the section numbers given here correspond to those used in NUREG-0700. Note that there may be minor editorial differences between the text in this appendix and the guidance in NUREG-0700, Revision 3. The term "applicants" in NUREG-0700 refers to those who prepare licensing submittals for NRC review.

B.5 Review Guidance for Degraded HSI and I&C Conditions Design Process

B.5.1 Operating Experience Review

(1) Applicants should review operating experience to identify the effects of failure modes and degraded conditions of the human-system interface (HSI) and instrumentation and control (I&C) subsystem on personnel performance.

Additional Information: Review Criterion 4 in Section 3, "Operating Experience Review," of NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," issued November 2012, identifies topics to be included in the review and in interviews with plant personnel. They include instrument failures, including system logic and control units; HSI equipment and processing failures (e.g., loss of video display units (VDUs) or of data processing); and transients, such as a loss of power to selected buses or the control room's power supplies. This guideline generalizes the NUREG-0711 criterion to the entire I&C system.

General knowledge from operating experience with digital I&C (DI&C) systems that relates to HSIs and personnel performance is limited. Thus, applicants should proactively seek this information for I&C designs that are similar to their own and use it as input to their human factors engineering (HFE) program.

B.5.2 Task Analysis

(1) The applicant's task analysis should identify the task requirements for managing HFE-significant HSI and I&C degradations so that risk-important tasks can be performed.

Additional Information: Task analysis is the means by which the task requirements for managing I&C degradations are identified. Those requirements are needed to define the features of the HSI design that support operators in monitoring and responding to such degradations. The analysis should also include tasks associated with failure and transition to backup systems; for example, transitioning to paper procedures upon failure of a computer-based procedure system.

(2) Applicants should determine the necessary compensatory actions and supporting procedures required to ensure that personnel can effectively manage the HFE-significant I&C degradation and the transition to backup systems.

Additional Information: Managing I&C degradations requires more than good HSIs. The actions to be taken must be analyzed, and the need for procedural support also determined to help operators manage the condition.

B.5.3 Treatment of Important Human Actions

(1) The applicant's probabilistic risk assessments (PRAs) and human reliability analyses (HRAs) should provide input to determining the impact of HFE-significant I&C degradations on human error and plant risk.

Additional Information: Recent approaches to HRA recognize the importance of the potential impact of sensor failure on the operator's situation assessment and, in turn, the effect of incorrect ones on errors of commission (e.g., Kim et al., 2005, 2008; NRC, 2000). For example, A Technique for Human Event Analysis (ATHEANA) recognizes the importance of situation assessment on human action and error (NRC, 2000). Factors leading to faulty assessments, including sensor failures, are identified as part of the analysis. This leads to efforts to predict errors of commission resulting from poor situational assessment. ATHEANA's HRA methods are useful in the current context, in that they suggest possible approaches to analyzing sensor degradations to identify those that might lead to incorrect situation assessments.

The analyses will support the applicant's efforts to address the staff's interim staff guidance in DI&C-ISG-03, "Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments," dated August 11, 2008 (NRC, 2008). The guidance notes that human errors associated with DI&C system failures have become more important contributors to core damage frequency and highlights the following considerations that applicants should address in their PRAs:

- Evaluate the acceptability of how the failure of control room indication is modeled.
- Assess the acceptability of the recovery actions taken for a loss of DI&C functions. If recovery actions are modeled, they should consider loss of instrumentation and the time available to complete such action. For guidance, refer to Regulatory Guide 1.200, Revision 2, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," issued March 2009 (NRC, 2009a), and HRA good practices in NUREG-1792, "Good Practices for Implementing Human Reliability Analysis," issued April 2005 (NRC, 2005).
- Ensure that, for self-testing and diagnostic features, the PRA accounts for the possibility that the system does not reconfigure itself after detecting a failure. Also, a diagnostic feature may not detect all of the failure modes, but only those it was designed to discover.
- If a communication network is shared, the effects on all systems because of failures of the network should be modeled jointly. The impact of communication faults on the related components or systems should be evaluated.
- Interactions within a DI&C system should be considered (multitasking, multiplexing).

B.5.4 Human-System Interface Design

(1) Applicants should conduct analyses to identify HFE-significant I&C degradations (i.e., the failure modes and degraded conditions of the I&C system) that could potentially affect the HSIs used by personnel in carrying out important human actions.

Additional Information: There are three key points in this review guideline: (1) analysis of the effects of I&C degradations on HSIs and personnel performance, (2) evaluation of degraded conditions in addition to complete failure, and (3) focusing the analysis on the impacts on operations. Each is discussed below.

While applicants typically analyze the effect of I&C failure modes and degradations on key plant systems, they do not expand it routinely to HSIs and personnel performance. For example, one study found that extending a designer's failure modes and effects analysis to include how the failures affect the HSIs can identify potential human performance impacts that can be addressed in system design. The ways in which resources, such as computer-based procedures and other HSIs, can degrade should be analyzed and understood fully so that they can be addressed within the HFE program to ensure that personnel perform risk-important tasks correctly.

Attention should be paid to degradations, not just complete failure. Complete failure, such as that of a computer-based procedures system, is easily recognized, and existing guidance already specifies the need for a backup system. More subtle degradations may be hard to discern yet may affect the information provided by HSIs and, thus, personnel performance.

Because of the very large number of HSIs in modern nuclear power plants, analyzing all of them may be impractical. Thus, evaluations may be applied in a graded fashion, by identifying the more important human actions and the HSIs most closely related to plant safety. Many lower-level DI&C failures that occur do not affect I&C system functionality from an operations perspective; maintenance personnel resolve them as part of their normal activities. The key in this guideline is identifying those degradations that lower the ability of personnel to monitor, detect, and assess situations, plan responses, and implement responses associated with important tasks. For example, the potential degradation of a DI&C system power supply should be analyzed because it is likely to affect the HSI.

The effects of instrumentation failures on graphic displays should be carefully analyzed. Potential failure problems should be evaluated in the context of the following questions:

- Can operators detect a failure of instrumentation?
- Can instrument failures result in representations that operators interpret as real process failures? Perhaps more important, can such process failures be misinterpreted as instrument failures?
- If operators detect a failure, should use of the display be suspended?
- Since the display may integrate many parameters into a single visualization, what effect does its loss have on operations, and how effectively can operators transition to backup displays?

This guidance is consistent with that in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations" (IEEE, 2003), specifying that a hazard analysis be undertaken to identify conditions that are not identified by the normal design review and testing process: "The hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems." Section D.4.2.3.2 states that techniques, such as fault tree analysis and failure modes and effects analysis, can be used to determine hazards. Section D.4.2.4.4 of this standard acknowledges that "the system-level impact of a hazard may be subtle, such as the display of an erroneous value that subsequently causes an operator to take an inappropriate action."

(2) Applicants should analyze the impacts of HSI and I&C degradations to ensure that they are not displayed in HSIs in ways that personnel will confuse with other process disturbances.

Additional Information: One concern about HSI and I&C degradations, particularly of the sensor and monitoring subsystem, is that they can (1) render displays difficult to interpret, and (2) perhaps worse, can make displays look as though a process disturbance has occurred. Analyses during the design process will help ensure that their effects are understood and the opportunity for misleading operators is minimized. The literature includes a variety of approaches to resolving this concern, including HRA (NRC, 2000), confusion matrices (Kim and Seong, 2008), and misdiagnosis tree analysis (Kim et al., 2005, 2008).

The analyses conducted for this guideline will support the applicant's ability to address the issues in DI&C-ISG-04, Revision 1, "Highly-Integrated Control Rooms—Communications Issues (HICRc)," dated March 6, 2009 (NRC, 2009b). Section 3.2 of DI&C-ISG-04, "Human Factors Considerations," cites the potential for providing operators with obsolete or erroneous information without advising them of potential inaccuracies. It states that applicants should demonstrate that they have considered these kinds of issues.

The guidance is also consistent with IEEE Std. 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (IEEE, 1998), and IEEE Std. 497-2016, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations" (IEEE, 2016). IEEE Std. 603-1998 states, "The design of the information display system shall minimize the possibility of ambiguous indications that could be confusing to the operator." IEEE Std. 497-2016, Section 6.5, "Information Ambiguity," states, "the failure of an accident monitoring instrument channel shall not result in information ambiguity that could lead the operator to defeat or fail to accomplish a required safety-related function", and it also states, "If analysis shows that credible failures can result in information ambiguity, a signal validation technique should be employed. If the signal validation process cannot be automatically accomplished, additional information shall be provided to allow the operators to deduce the actual conditions so that they may properly perform their role."

(3) Applicants should determine the alarms and the information personnel need to detect HFE-significant I&C degradations promptly and to identify the extent and significance of the condition.

Additional Information: This information is an essential input to designing HSIs that will be effective in supporting operators in the detection and management of degraded conditions.

(4) Applicants should determine the necessary backup systems, if any, needed to ensure that risk-important tasks can be performed.

Additional Information: Depending on the extent of redundancy and diversity in the I&C systems involved and the type of support given to operators, backup systems may be necessary. For example, if there is a major loss of DI&C, a backup may be needed to manage safety functions.

B.5.5 Training Program Development

(1) Operator training programs should support personnel in the following ways:

- understanding how and why the HSIs and I&C subsystems might degrade or fail
- knowing the implications of such degradations for HSI and their own task performance
- monitoring the I&C system's performance, so degradations and failures are detected and recognized through the control room HSIs (e.g., recognizing display format failure modes and effects on the graphical presentation)
- performing recovery actions and compensatory actions in the event of degraded conditions
- determining when to override degraded systems
- smoothly transitioning to backup systems when needed and returning when system functions are restored
- comprehending how the roles and responsibilities of crew members and the concept of operations will be affected by degraded HSI and I&C conditions

Additional Information: Operator training plays an important role in supporting operators who detect degradations and in understanding the types of degraded conditions that can occur. For example, for failures of automatic systems, classroom learning and on-the-job training are enhanced by simulator training that specifically provides operators with experience of different failures (O'Hara and Higgins, 2010).

B.5.6 Human Factors Verification and Validation

(1) HFE-significant I&C degradations should be addressed by integrated system validation to ensure that measures taken in designing HSIs, developing procedures, and training operators will successfully mitigate the potential effects of these conditions on personnel performance of risk-important tasks.

Additional Information: This guidance is a more complete treatment of HSI and I&C degradations than exists in the current guidance. As part of the sampling of operational conditions, NUREG-0711, Revision 3, Section 11.4.1.1, "Review Criterion 1," identifies "I&C and HSI failures and degraded conditions" as a sampling dimension. This guideline

provides more information about the aspects of these conditions that should be considered in validation.

B.6 References

Institute of Electrical and Electronics Engineers (IEEE) (1998). “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (IEEE Std. 603-1998). New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (2003). “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (IEEE Std 7-4.3.2-2003) , New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (2004). “IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities” (IEEE Std. 1023-2004). New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (2016). “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations” (IEEE Std. 497-2016). New York, NY: Institute of Electrical and Electronics Engineers.

Kim, J., W. Jung, and J. Park (2005). “A systematic approach to analyzing errors of commission from diagnosis failure in accident progression.” *Reliability Engineering and System Safety*, 89, 137–50.

Kim, J., W. Jung, and Y. Son (2008). “The MDTA-based method for assessing diagnosis failures and their impacts in nuclear power plants.” *Reliability Engineering and System Safety*, 93, 337–349.

Kim, M., and P. Seong (2008). “A method for identifying instrument faults in nuclear power plants possibly leading to wrong situation assessment.” *Reliability Engineering and System Safety*, 93, 316–324.

O’Hara, J., and J. Higgins (2010). “Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis” (BNL-91017-2010). Upton, NY: Brookhaven National Laboratory.

U.S. Nuclear Regulatory Commission (2000). “Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)” (NUREG-1624, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, May.

U.S. Nuclear Regulatory Commission (2005). “Good Practices for Implementing Human Reliability Analysis (HRA)” (NUREG-1792). Washington, DC: U.S. Nuclear Regulatory Commission, April.

U.S. Nuclear Regulatory Commission (2008). “Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments: Interim Staff Guidance” (DI&C-ISG-03, Rev. 0). Washington, DC: U.S. Nuclear Regulatory Commission, August 11. (ML080570048)

U.S. Nuclear Regulatory Commission (2009a). “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities” (Regulatory Guide 1.200, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission, March.

U.S. Nuclear Regulatory Commission (2009b). “Highly-Integrated Control Rooms—Communications Issues (HICRc)” (DI&C-ISG-04, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission, March 6. (ML083310185)

APPENDIX C GLOSSARY

The following definitions were included in the glossary of NUREG-0700, Revision 3, "Human-System Interface Design Review Guidelines," issued July 2020.

Analytical redundancy—The calculation of expected parameter values using a model of system performance. For example, "reactor power," "reactor coolant temperature rise through the reactor core," and "reactor coolant flow rate" are interrelated parameters based upon the physical principles of heat transfer. A measured value for coolant flow should be consistent with the analytically calculated value for coolant flow determined from the corresponding measured values of reactor power and coolant temperature rise.

Architecture—The organizational structure of a system.

Degraded condition—A state in which a system or component operates at less than its fully intended function, including failure.

Derived information—Displayed information that could be based directly on sensor measurement but instead is derived from the measurements of other sensors. For example, the flow into a tank might not be directly sensed but can be assessed from a change in level over time. (See also directly sensed and synthetic information.)

Directly sensed information—Information that is derived from a sensor measurement (e.g., the flow out of a tank based on a flow sensor in the output pipe. (See also derived and synthetic information.)

Failure—Inability of a system or component to perform its function.

Fault tolerance—The existence of redundancy or diversity with fault-detection capability. Continuity of operations is ensured by providing the needed function using a capability that is fault-free.

HFE-significant I&C degradations—The failure modes and degraded conditions of the I&C system that have the potential to affect HSIs used by personnel in performing important human actions (defined below).

Important human actions—Important HAs [human actions] consist of those actions that meet either risk or deterministic criteria:

- **Risk-important human actions**—Actions defined by risk criteria that plant personnel use to ensure the plant's safety. There are absolute and relative criteria for defining risk-important actions. For absolute ones, a risk-important action is any action the successful performance of which is needed to reasonably ensure that predefined risk criteria are met. For relative criteria, the risk-important actions are defined as those with the greatest risk compared to all human actions. The identifications can be made quantitatively from risk analyses, and qualitatively from various criteria, such as concerns about task performance based on considering performance-shaping factors.

- **Deterministically identified important human actions**—Deterministic engineering analyses typically are completed as part of the suite of analyses in the final safety

analysis report or design control document in Chapters 7, “Instrumentation & Controls,” and 15, “Transient and Accident Analyses.” These deterministic analyses also often credit human actions.

Redundancy—In fault tolerance, the presence of auxiliary components in a system to perform the same or similar functions as other components with the purpose of preventing or recovering from failures.

Signal validation—A set of processing techniques by which signals, such as alarm signals, from redundant or functionally related sensors are compared and analyzed to determine whether a true alarm condition exists. The purpose of these techniques is to prevent false alarms being presented to the operator because of malfunctioning plant instrumentation, such as a failed sensor.

Synthetic information—Information that represents higher order information about a plant that cannot be sensed directly but is computed mathematically from data gained from sensors (e.g., rate of change, mass balance). The overall status of a safety function may represent synthetic information based on a computation from the function’s key safety parameters. Any such data used in these calculations from degraded or faulty sensors may propagate to the synthetic parameter and distort its meaning (see also directly sensed and derived information).

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-7264
BNL-228841-2025-NREG

2. TITLE AND SUBTITLE

Managing the Effects of Degraded Digital Instrumentation and Control Conditions on Operator Performance

Human Factors Engineering Review Guidance Development

3. DATE REPORT PUBLISHED

MONTH	YEAR
December	2025

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

J. O'Hara, W. Gunther, G. Martinez-Guridi, T. Anderson, J. Xing, S. Morrow

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Brookhaven National Laboratory
Nuclear Science & Technology Department
P.O. Box 5000
Upton, NY 11973

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

Jing Xing and Stephanie Morrow, NRC Project Managers

11. ABSTRACT (200 words or less)

Modern digital instrumentation and control (DI&C) systems provide sophisticated monitoring, diagnostic, and prognostic functions, as well as integrated control of plant systems and processes. Personnel interact with DI&C systems through human-system interfaces (HSIs) in the control room and elsewhere in a nuclear power plant. While digital systems are generally reliable, their potential degradation or failure could affect operator performance and consequently impact plant safety. The objectives of this U.S. Nuclear Regulatory Commission (NRC) research were to (1) examine the effects of degraded HSI and DI&C conditions on human performance and plant operations, and (2) develop guidance for the review of HSI support for the detection and management of degraded HSI and DI&C conditions by plant personnel. The study followed the NRC's methodology for the development of human factors engineering guidance, which consists of four steps: (1) user needs analysis, (2) technical basis and guidance development, (3) peer review, and (4) guidance integration and document publication. The technical basis was established from a review of pertinent standards and guidelines, empirical studies, plant operating experience, and DI&C failure events. The guidance in this report was incorporated into NUREG-0700, Revision 3, "Human System Interface Design Review Guidelines," issued July 2020.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Human Factors Engineering (HFE); Human-System Interfaces (HSI); Digital Instrumentation and Control; Operator Performance; Safety Parameter Display System; Nuclear Safety; Human Actions

13. AVAILABILITY STATEMENT

unlimited

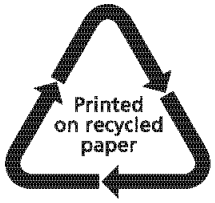
14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG/CR-7264

Managing the Effects of Degraded Digital Instrumentation and Control Conditions on Operator Performance

December 2025